MASON
consulting

AI時代のサプライチェーン防衛：事業を支える強靭なサプライチェーンセキュリティ構築の戦略

2024年11月20日

メイソンコンサルティング株式会社

藤田 哲矢

メイソンコンサルティング株式会社 代表取締役

- 横浜国立大学経営学部卒業
- 一橋大学大学院商学研究科修了。
- INSEAD(欧州経営大学院)AMP修了。

- ソフトバンク、アクセンチュアを経てメイソンコンサルタントグループに入社。その後、分社化をしてメイソンコンサルティングを設立。
- 製造業、ハイテク業のお客様を中心に業務プロセス・テクノロジー領域のコンサルティング、監査業務を実施。
- 直近においては、欧州を中心にしたグローバルなサイバーセキュリティコンソーシアムのタスクフォースの活動でサプライチェーンセキュリティを牽引。

社名	メイソンコンサルティング株式会社 （英文名：Mason Consulting Co., Ltd）
設立	2017年10月
代表	代表取締役　藤田　哲矢
事業内容	コンサルティング、ISO取得・運用、各種セキュリティサービス ・サイバーセキュリティ診断・コンサルティング ・ISO・セキュリティ認証取得コンサルティング ・ISO・セキュリティ運用アウトソーシング ・プロジェクトマネジメントサービス ・リスクマネジメントコンサルティング
所属団体	・サプライチェーンセキュリティコンソーシアム(SC3) ・クラウドセキュリティアライアンスジャパン(CSA)
連絡先	TEL：03-6425-6735 Eメール：info@mason-c.co.jp
住所	〒105-0012 東京都港区芝大門1-10-11 芝大門センタービル10F

MASON consulting

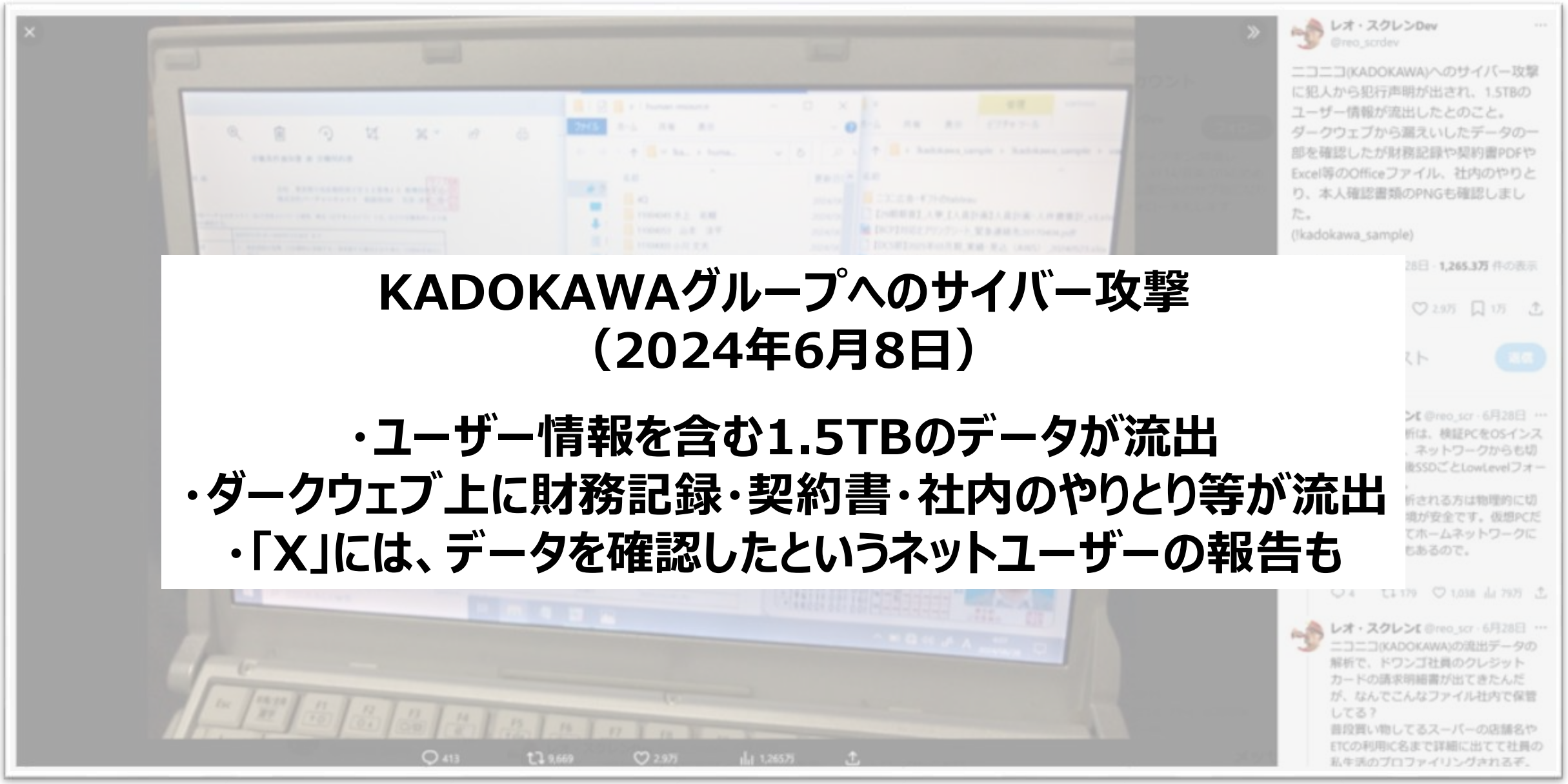
アクセス

山手線・京浜東北線『浜松町』駅　徒歩7分
都営浅草線・大江戸線『大門』駅　徒歩3分
都営三田線『御成門』駅　徒歩2分

取引実績
(一部・順不同)

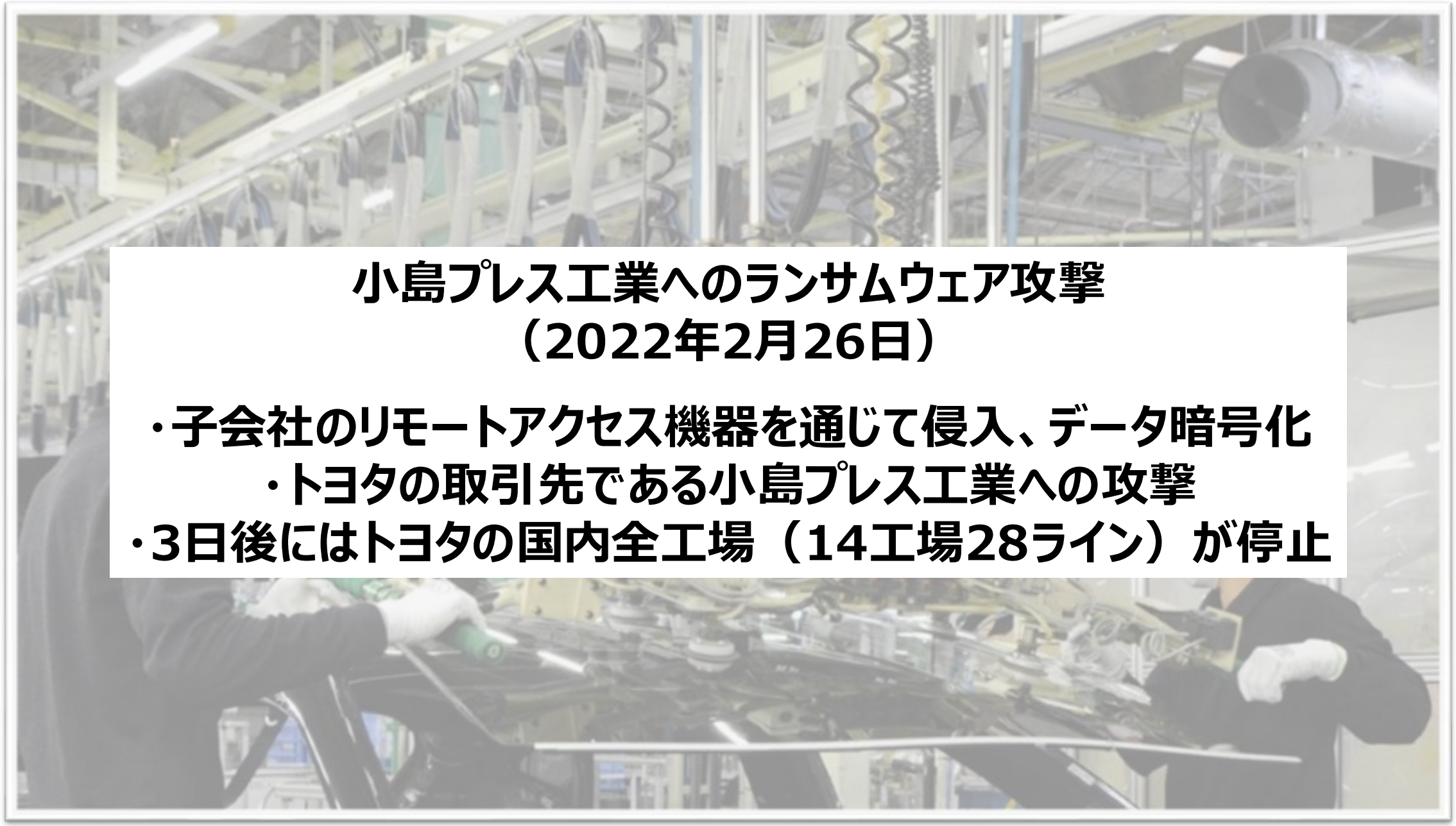
NTT DATA　accenture　NC network 挑戦する製造業のために　UNIADEX　SoftBank

J:COM　AIDEM　MITSUBISHI PAPER MILLS LIMITED　JOCA 公益社団法人 青年海外協力協会　など多数



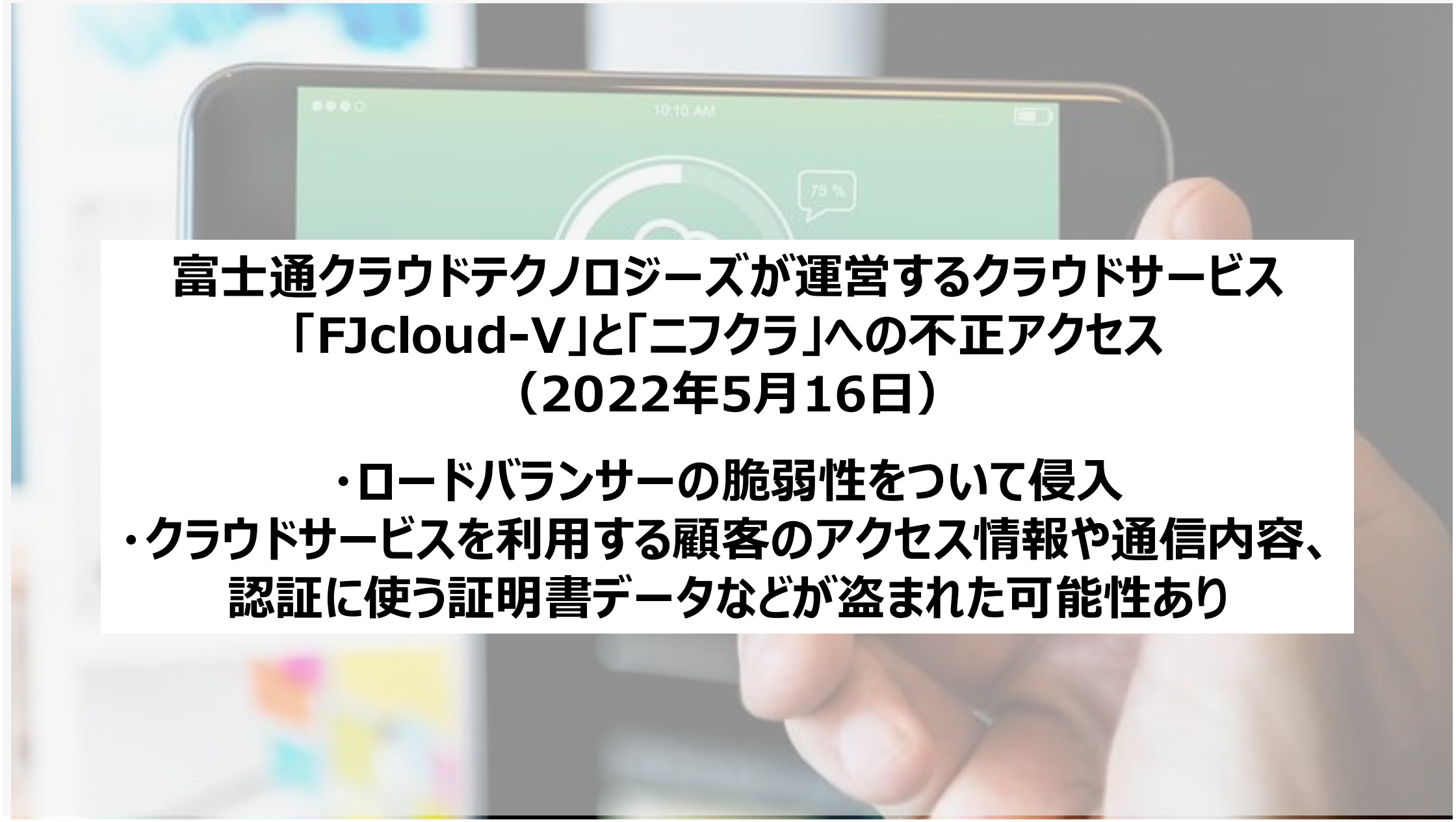
KADOKAWAグループへのサイバー攻撃
（2024年6月8日）

・ユーザー情報を含む1.5TBのデータが流出
・ダークウェブ上に財務記録・契約書・社内のやりとり等が流出
・「X」には、データを確認したというネットユーザーの報告も



小島プレス工業へのランサムウェア攻撃
（2022年2月26日）

・子会社のリモートアクセス機器を通じて侵入、データ暗号化
・トヨタの取引先である小島プレス工業への攻撃
・3日後にはトヨタの国内全工場（14工場28ライン）が停止



富士通クラウドテクノロジーズが運営するクラウドサービス「FJcloud-V」と「ニフクラ」への不正アクセス（2022年5月16日）

・ロードバランサーの脆弱性をついて侵入
・クラウドサービスを利用する顧客のアクセス情報や通信内容、認証に使う証明書データなどが盗まれた可能性あり

世の中での被害事例

主なリスク	分類	発生組織	被害の概要
業務停止	ランサムウェア サプライチェーン	自動車部品製造メーカ （小島プレス工業）	サプライチェーン 2022年2月、自社で発生したランサムウェア攻撃に起因 取引先である自動車製造メーカー（トヨタ自動車）へ波及、**国内全工場（14工場28ライン）停止**。
機密情報・個人情報漏洩	不正アクセス	通信サービス （富士通クラウドテクノロジーズ）	2022年5月、運営するクラウドサービスにロードバランサーの脆弱性をついて不正アクセスあり。**クラウドサービスを利用する顧客のアクセス情報や通信内容、認証に使う証明書データなどが盗まれた可能性あり**。
業務停止	ランサムウェア	関西地方の総合医療セン （大阪急性期総合医	サプライチェーン 2022年10月、総合医療センターがランサムウェア攻撃 **緊急以外の手術や外来診療を停止**。
業務停止 機密情報・個人情報漏洩	ランサムウェア サプライチェーン	出版 （KADOKAWAグループ）	サプライチェーン 2024年6月、グループ会社のデータセンターのサーバがサ 攻撃を受け、システム障害が発生、**グループ全体の事業に影響**、従業員個人情報の他、取引先との契約書、学校法人の生徒の個人情報などが漏洩。
機密情報・個人情報漏洩	ランサムウェア サプライチェーン	通信サービス	サプライチェーン 2023年11月、サーバがサイバー攻撃を受け**約44万件** **情報が流出**、さらに2024年2月にも**従業員情報約57,000件が流出した可能性あり**。
機密情報・個人情報漏洩	標的型攻撃 サプライチェーン	電機製造	サプライチェーン 2020年1月、11月、翌年10月と相次いで中国現法へ アクセスを契機とした情報漏洩が発生。**漏洩した情報には、防衛関連情報20,000件が含まれ、安全保障への影響も懸念される**。

参考資料：一般社団法人日本自動車工業会および一般社団法人日本自動車部品工業会. 2024年度経営層向け説明会資料「自動車産業サイバーセキュリティガイドライン」自己評価実施・展開のお願い. https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_supply_chain_briefing_material_20240913.pdf, 2024年11月18日閲覧.

日経XTECH

ハッカーに狙われたトヨタ、小島プレスへの攻撃で国内全工場停止

日経XTECH

大阪の病院は取引業者からランサムウエアがなぜ広がった？「攻撃の横展開」に注意

Bloomberg

日本で急増するサイバー攻撃、世界

朝日新聞 DIGITAL

サプライチェーンを狙ったサイバー攻撃は
日々ニュースに取り上げられています。

トヨタの工場を止めたサイバー攻撃　サプライチェーン攻撃のリスクが露呈

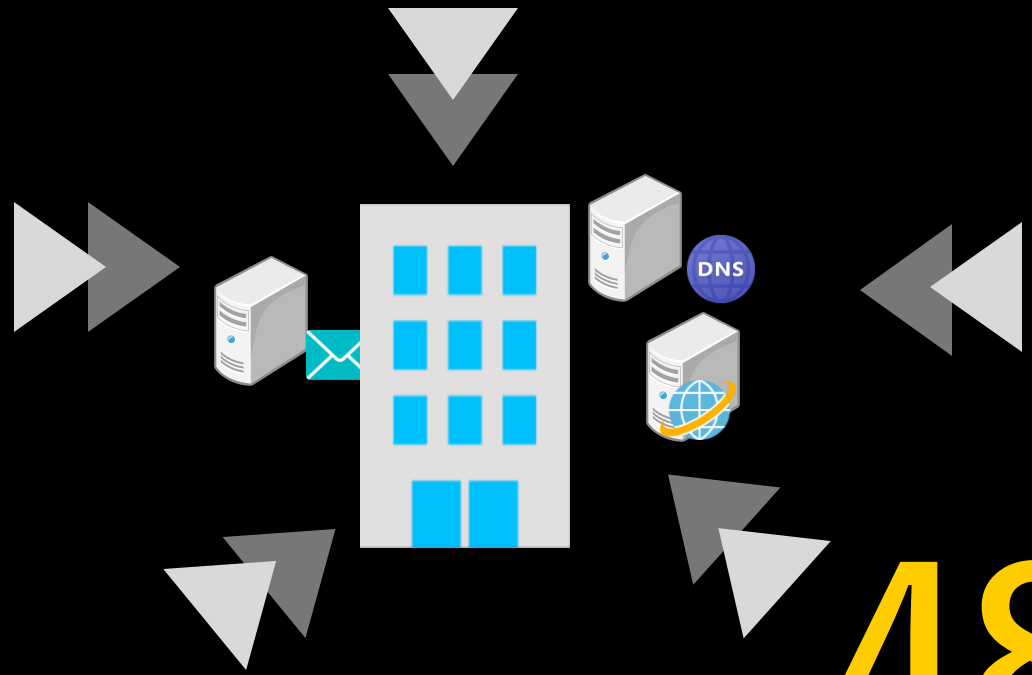
2022.03.14

トヨタ自動車のサプライチェーン（供給網）に連なる小島プレス工業がマルウエア被害を受けた。これがきっかけで、トヨタの14工場の28ラインが止まった。かねて指摘されていた「サプライチェーン攻撃」のリスクと被害の大きさが浮き彫りになった。

サイバー攻撃の現状(平均)

3.75時間
侵入から攻撃展開するまでの平均*2

397日
サイバー攻撃発生から公表するまでの平均*1



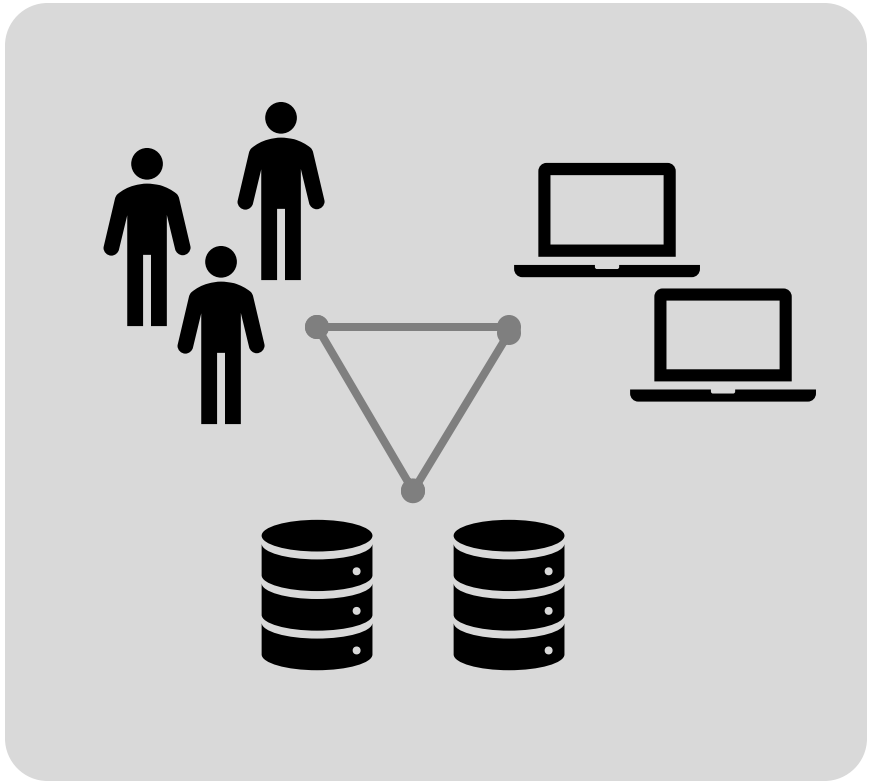
63%
外部からサイバー攻撃を指摘される割合*3

913グループ
新たに追跡された攻撃グループ*3

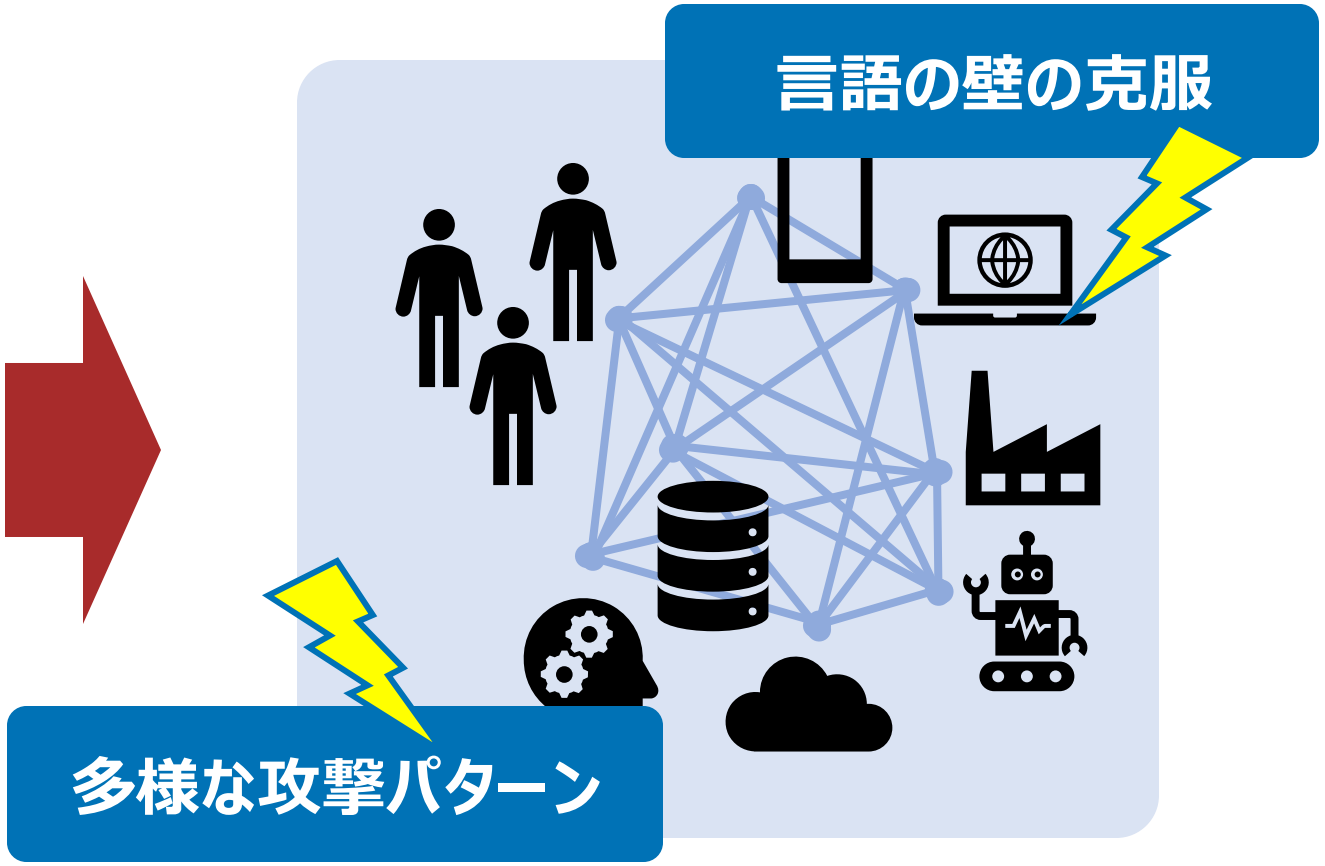
48%
金銭目的の攻撃グループの割合*3

＊1：サイバーセキュリティクラウドによる法人・団体における不正アクセスに関する被害規模の調査(2022年1月1日～2023年11月30日)
＊2：株式会社網屋主催の「Security BLAZE 2022」の解説
＊3：Google Cloudでセキュリティ事業を手がけるMandiantの年次報告書(2023年5月)

ITインフラ環境の発達に伴い、サイバー攻撃も多様化・高度化



自社で完結する、限られたシステム



クラウドを含む、複雑で多様なシステム

「サプライチェーン攻撃」は、情報処理推進機構（IPA）の「情報セキュリティ10大脅威」でも、「組織」向け脅威のカテゴリーで、2位にランクイン（2016年以降6年連続6回ランクイン）

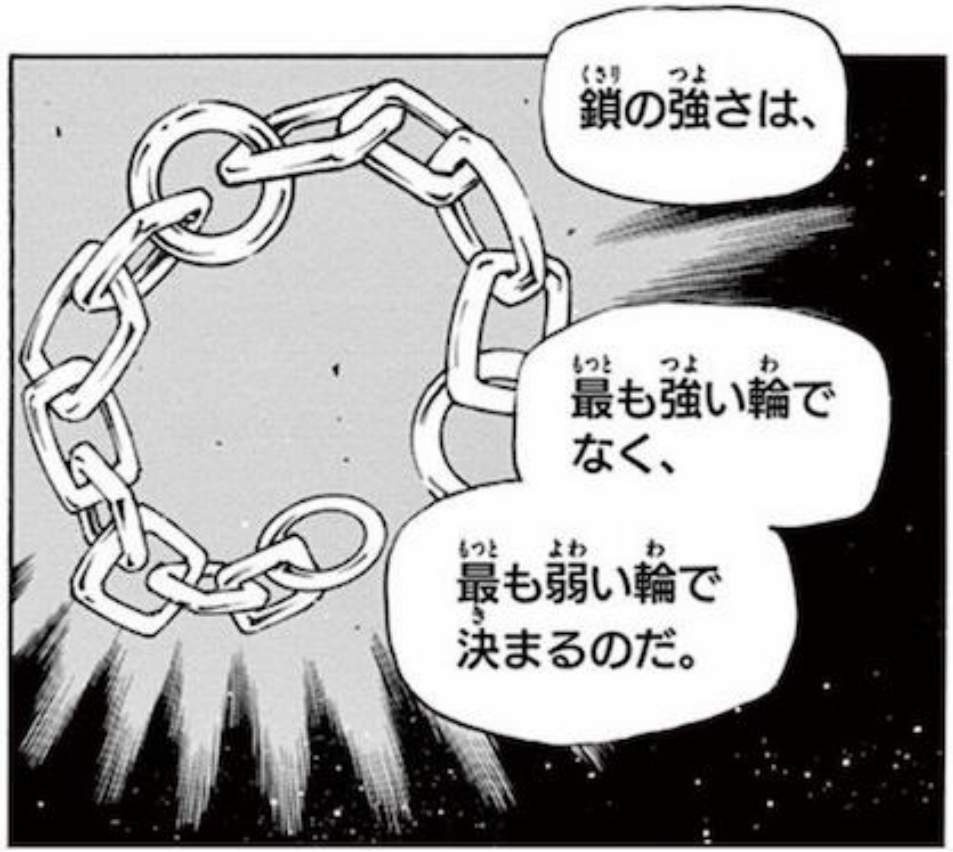
順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続9回目
2	**サプライチェーンの弱点を悪用した攻撃**	**2019年**	**6年連続6回目**
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

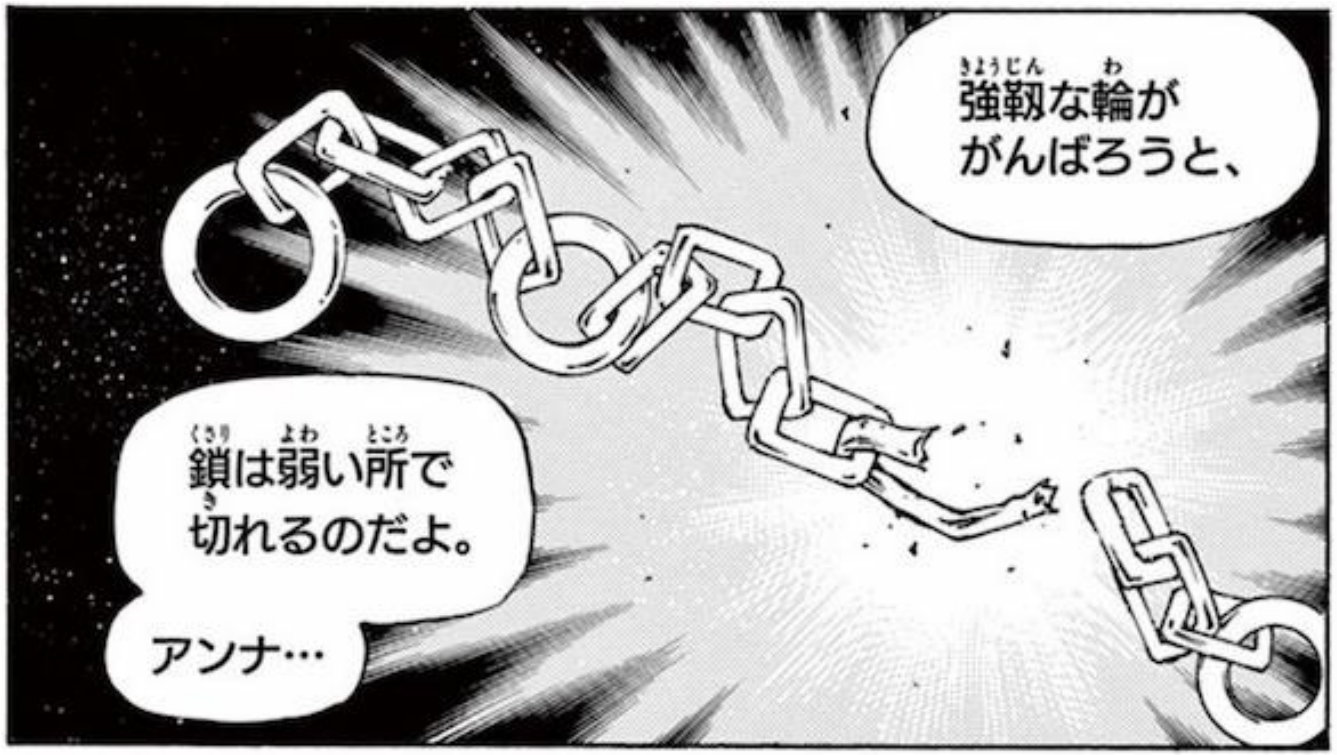
ビジネスサプライチェーン攻撃発生時、8割以上でシステム停止。

#	発覚／公表日時	業種／業界	被害	発覚原因	攻撃に使われた手口
1	2023年1月	運輸・交通・インフラ	情報漏えい	未公表	ネットワーク共有していたサーバに侵害
2	2023年1月	建設・不動産	障害発生（システム停止）,データ改ざん/破壊,情報漏えい	攻撃者による通知	ランサムウェア（Lockbit）
3	2023年1月	建設・不動産	障害発生（システム停止）,データ改ざん/破壊,情報漏えい	攻撃者による通知	ランサムウェア（Lockbit）
4	2023年1月	建設・不動産	障害発生（システム停止）,データ改ざん/破壊,情報漏えい	攻撃者による通知	ランサムウェア（Lockbit）
5	2023年1月	建設・不動産	障害発生（システム停止）,データ改ざん/破壊,情報漏えい	攻撃者による通知	ランサムウェア（Lockbit）
6	2023年1月	建設・不動産	障害発生（システム停止）,データ改ざん/破壊,情報漏えい	攻撃者による通知	ランサムウェア（Lockbit）
7	2023年1月	水産・農林・鉱業	障害発生（システム停止）,データ改ざん/破壊,情報漏えい	攻撃者による通知	ランサムウェア（Lockbit）
8	2023年1月	水産・農林・鉱業	障害発生（システム停止）,データ改ざん/破壊,情報漏えい	攻撃者による通知	ランサムウェア（Lockbit）
9	2023年1月	建設・不動産	障害発生（システム停止）,データ改ざん/破壊	攻撃者による通知	ランサムウェア（Lockbit）
10	2023年1月	製造	障害発生（システム停止）,データ改ざん/破壊	攻撃者による通知	ランサムウェア（Lockbit）
11	2023年1月	建設・不動産	障害発生（システム停止）,データ改ざん/破壊	攻撃者による通知	ランサムウェア（Lockbit）
12	2023年4月	製造	障害発生（システム停止）,情報漏えい	自己調査	ファイルサーバー侵害
13	2023年5月	医療	情報漏えい	未公表	海外アカウント経由のクラウドプラットフォームへの侵害
14	2023年7月	製造	情報漏えい,障害発生（システム停止）	自己調査	なりすまし

国内で公表されたビジネスサプライチェーン攻撃の被害事例　（2023年1月～2023年10月までの公表事例をトレンドマイクロが整理）
https://www.trendmicro.com/ja_jp/jp-security/23/k/securitytrend-20231113-01.html

サプライチェーンセキュリティの重要性





週刊少年サンデー連載『BE BLUES!～青になれ～』第82節 連鎖するパス より

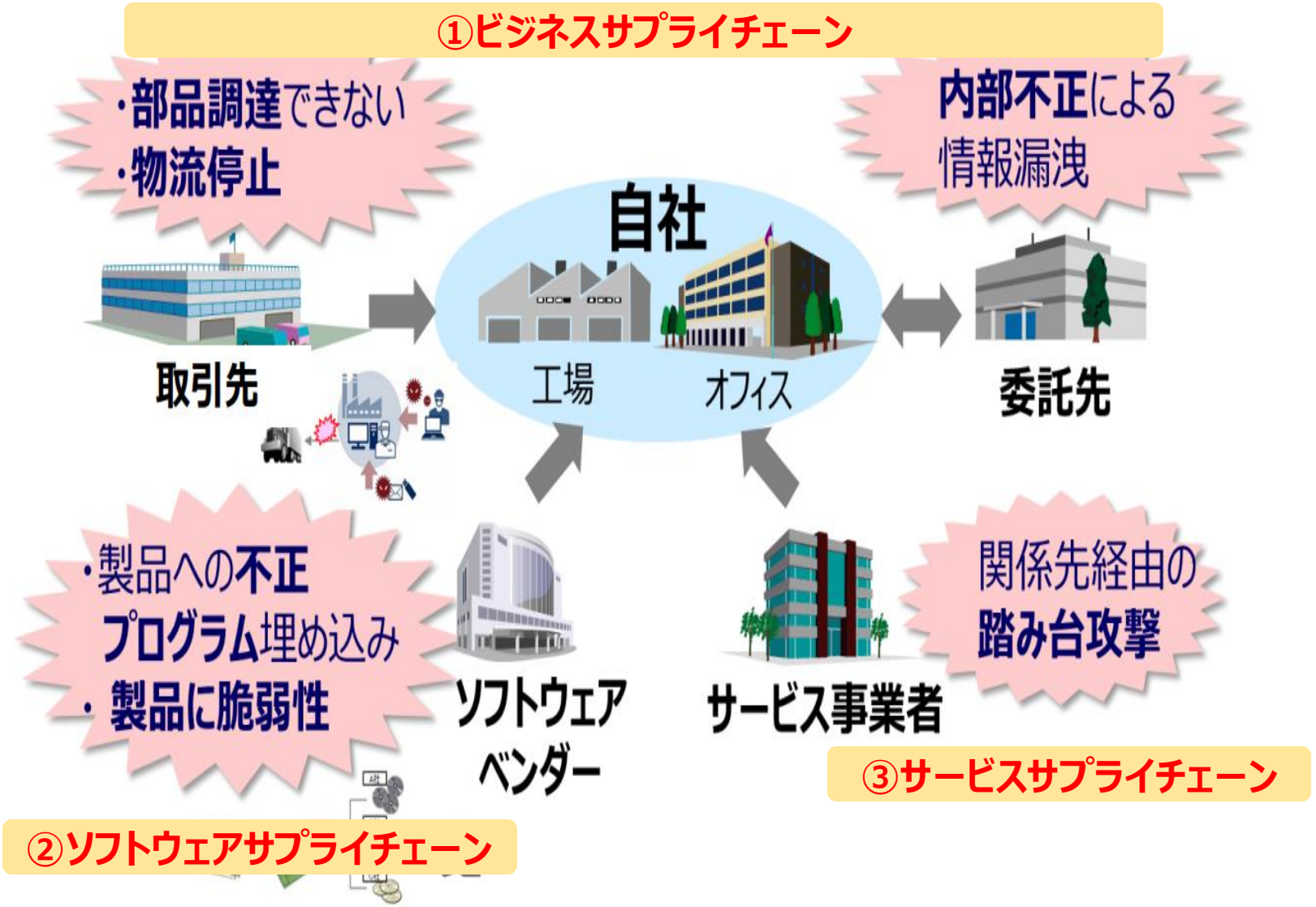
サプライチェーンセキュリティの重要性

「鎖の強さは、一番弱い輪によって決まる」
十八世紀の英哲学者リードが書いた言葉。

弱いところが攻撃されると
全体に影響してしまう。

サイバーセキュリティにおいて、攻撃者は常に弱い部分を狙っており、サプライチェーン全体でのリスク管理が必要となっている。

多様なサプライチェーン攻撃

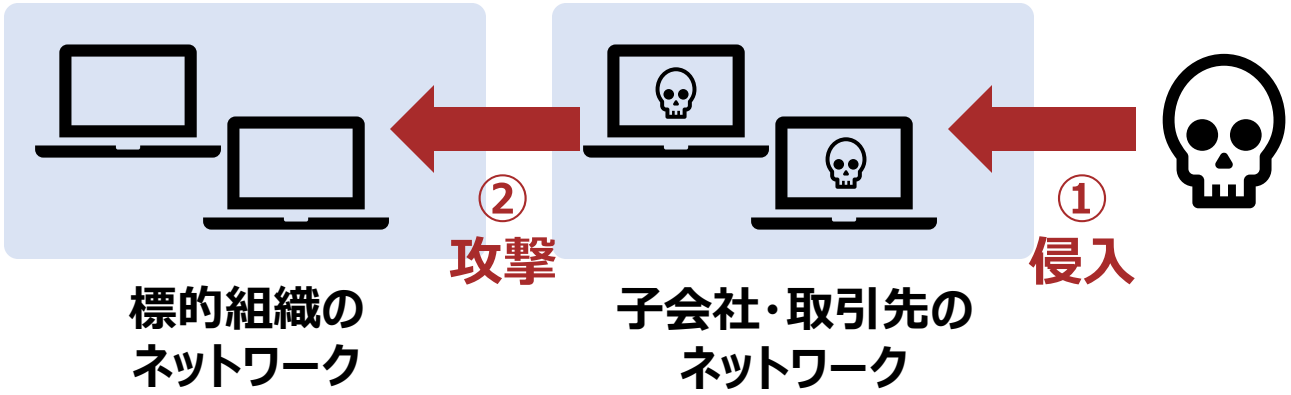


1. ビジネス サプライチェーン 攻撃
2. ソフトウェア サプライチェーン 攻撃
3. サービス サプライチェーン 攻撃

1

ビジネス サプライチェーン 攻撃

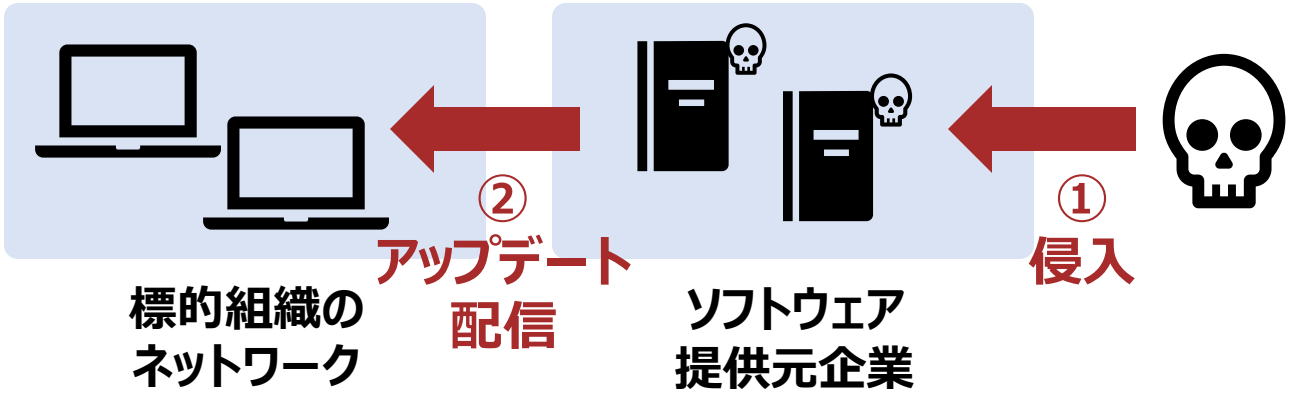
関連組織や子会社、取引先などを侵害し、
標的組織への侵害を図る攻撃



2

ソフトウェア サプライチェーン 攻撃

ソフトウェアそのものやアップデートプログラムなどに
不正コードを混入し、標的組織に侵入する攻撃



3

サービス サプライチェーン 攻撃

サービス事業者を侵害し、サービスを通じて
その顧客に被害を及ぼす攻撃

本日お伝えしたいこと

- サプライチェーンセキュリティ強化のため、
  まずは**評価サービスを使ってサプライヤーを「クイック診断」する**ことが望ましい。
- ただしクイック診断は万能ではないため、サプライヤと連携し、
  経営者主導で、必要なセキュリティ対策を追加で実施することが重要。
- 必要なセキュリティ対策の投資を意思決定するためには、
  投資対効果に基づいて経営層が意思決定する仕組みの構築が求められる。

大手企業のサプライチェーンセキュリティ課題

取引先を踏み台にした
攻撃に対して
備えがない

ビジネスインパクトの低い
取引先にセキュリティリスクは
無いのでは？

自社のセキュリティ対策に
比べて、取引先の
セキュリティ対策を軽視

取引先からのメールを
通じて
攻撃されるなんて、まさか・・・

中小企業のセキュリティ課題

そもそも
サイバーセキュリティ
って何？？

必要性は理解しているが
何から対策を
行えばよいのか・・・

自社の
セキュリティの弱みが
何かわからない

セキュリティ対策の
コストを
支払えない。

大手企業のサプライチェーンセキュリティ対策状況(現状)

何も
していない

ISO27001
取得を
求める

Excel等の
チェックリストで
モニタリング

ISO27001 取得を 求める

情報セキュリティに関する第三者認証の取得をサプライヤに求める手法。
日本国内では7,800社以上が取得。

ただし・・・
・サプライヤー全部が取得するにはコストがかかる。
・ISO27001は管理プロセスに対する認証のため、
　技術的対策への評価が十分ではない。

Excel等のチェックリストでモニタリング

取引先に対して、サイバーセキュリティ対策の状況をヒアリングするチェックリストを送付し、各社の対応状況を調査・把握する手法。

ただし・・・

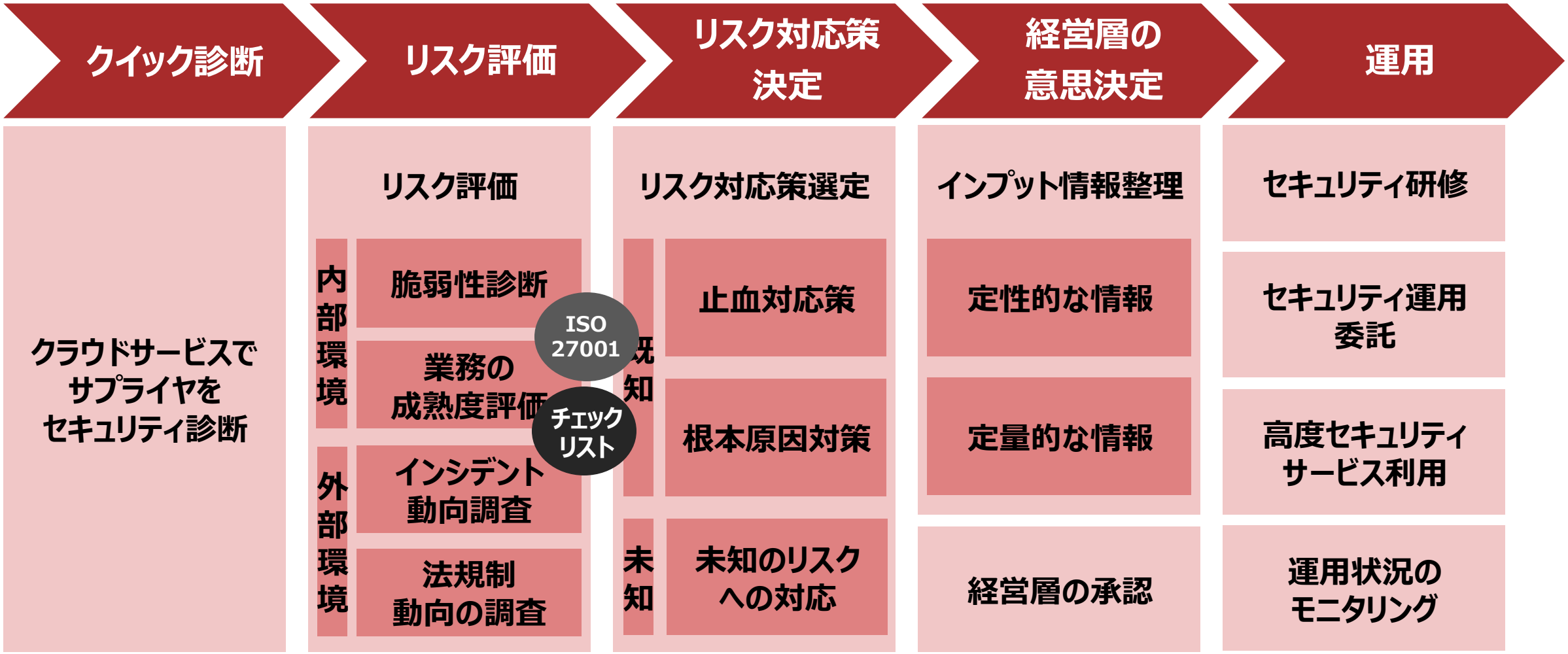
・Excelベースでの作業は手間が大きい。
・脆弱性診断など、外部からの検査のすべがない。
・詳細なフィードバックをするには限界がある。

サプライチェーンセキュリティの現状

本来はどうあるべきなのか？

サプライチェーンセキュリティ強化の全体像を
見据えてアクションすべき

サプライチェーンセキュリティ強化の全体像



まずは、セキュリティリスクの見える化から始めましょう

クイック診断 → リスク評価 → リスク対応策決定 → 意思決定 → 運用

クイック診断

クラウドサービスで
サプライヤを
セキュリティ診断

**まずは
ここから！**

リスク評価

内部環境
- 脆弱性診断
- 業務の成熟度評価

外部環境
- インシデント動向調査
- 法規制動向の調査

ISO 27001

チェックリスト

リスク対応策選定

- 止血対応策

**本来はセキュリティ監査
（脆弱性診断＋業務の成熟度評価）
をすべてのサプライヤに行うべきですが・・・**

**コストが現実的ではなく、
対象の重み付け・絞り込みも難しいです**

インプット情報整理

- 定性的な情報

セキュリティ研修

- セキュリティ運用委託
- 高度セキュリティサービス利用
- 運用状況のモニタリング

サプライヤの「クイック診断」が可能な
「セキュリティ評価ツール」の導入が広がっています

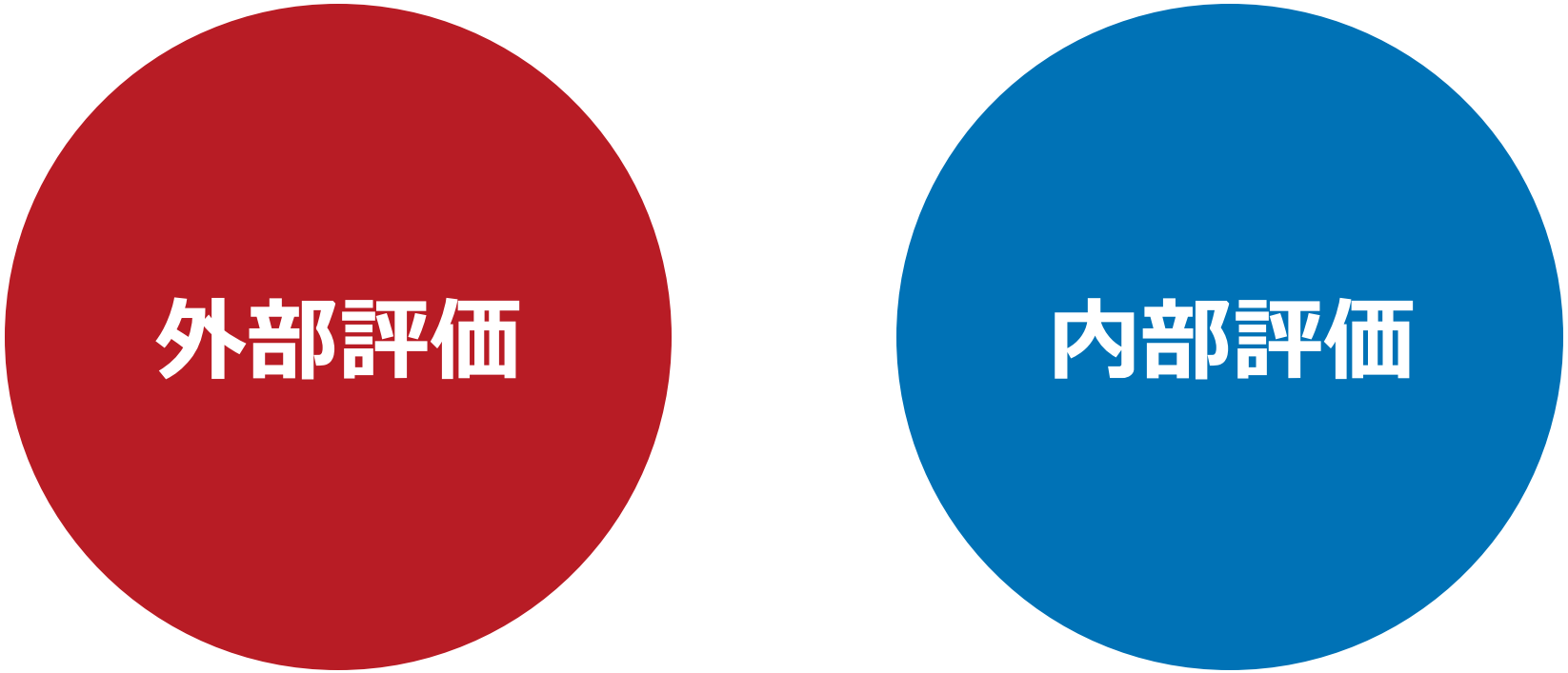
Panorays

DAIFUKU Automation that Inspires　JINS　KYB　KYOCERA 京セラ コミュニケーションシステム　MOTEX　OYO 応用地質株式会社

SOMPOリスクマネジメント Webページより
https://www.sompocybersecurity.com/service/panorays.html

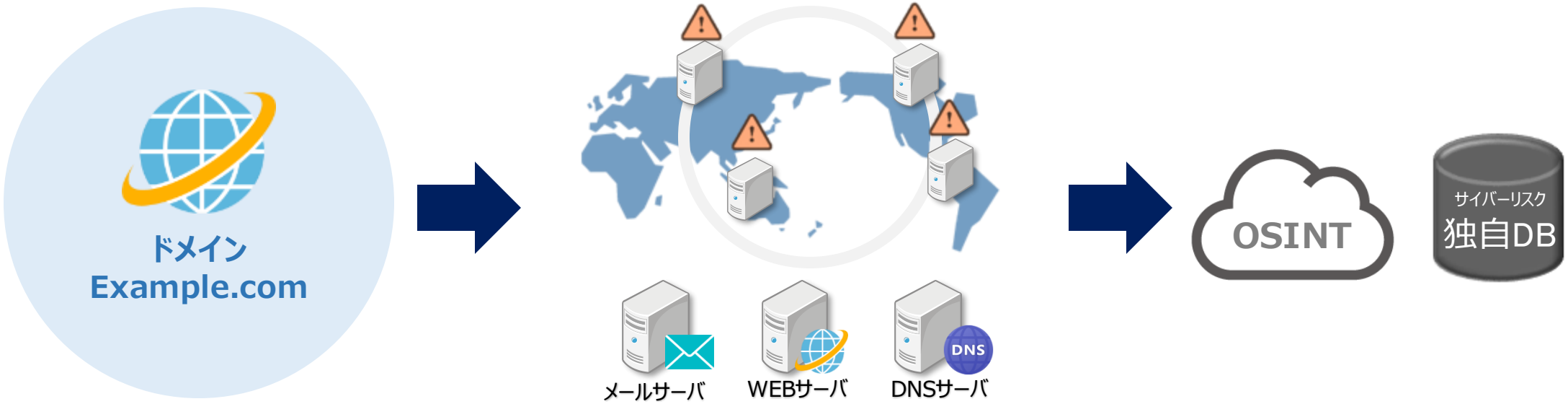
セキュリティ評価ツール「Panorays」は

セキュリティ版の「帝国データバンク」



外部評価

対象サプライヤーの
外部から見えるサイバーリスクを自動的に評価



対象サプライヤーの
ドメイン情報のみ

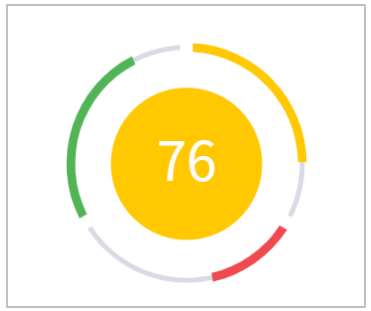
ドメインに紐づく外部公開アセットの
自動で定期的に収集・分析

収集した外部公開アセットに対して
OSINT情報やサービス独自DBを
もとにサイバーリスクを分析

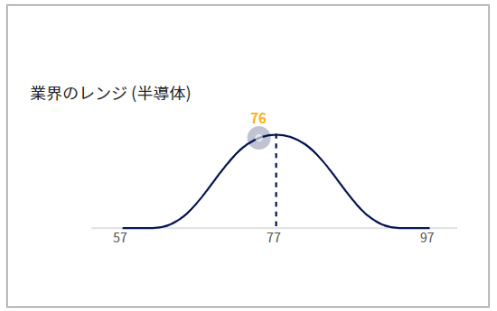
外部評価

対象サプライヤーの
外部から見えるサイバーリスクを自動的に評価

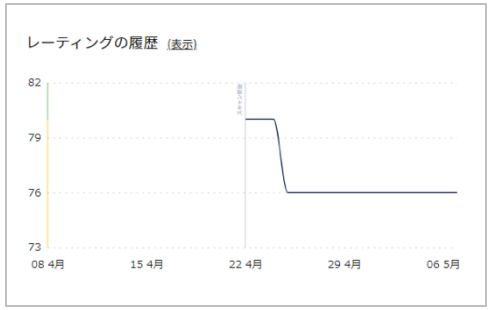
100点満点のスコア、業界比較による
客観的評価から具体的な対策に
必要な詳細情報まで表示



100点満点のスコア



同業種との比較



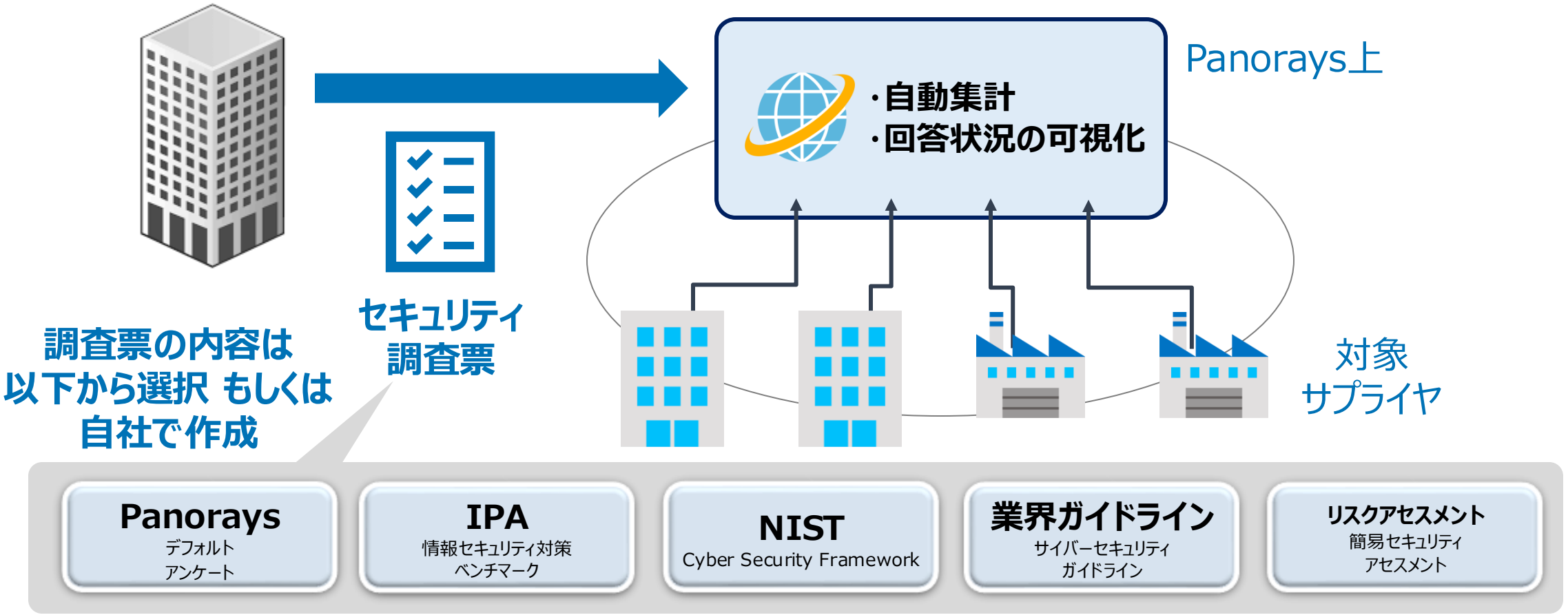
スコア履歴

検出されたサイバーリスクの対策支援

解説	**改善策**	**関連のCVE情報**
サイバーリスクの概要説明	サイバーリスクの対策方法を説明	サイバーリスクの詳細なリスク情報

内部評価

セキュリティ組織体制・対策状況のアンケートを オンラインで効率的に実施

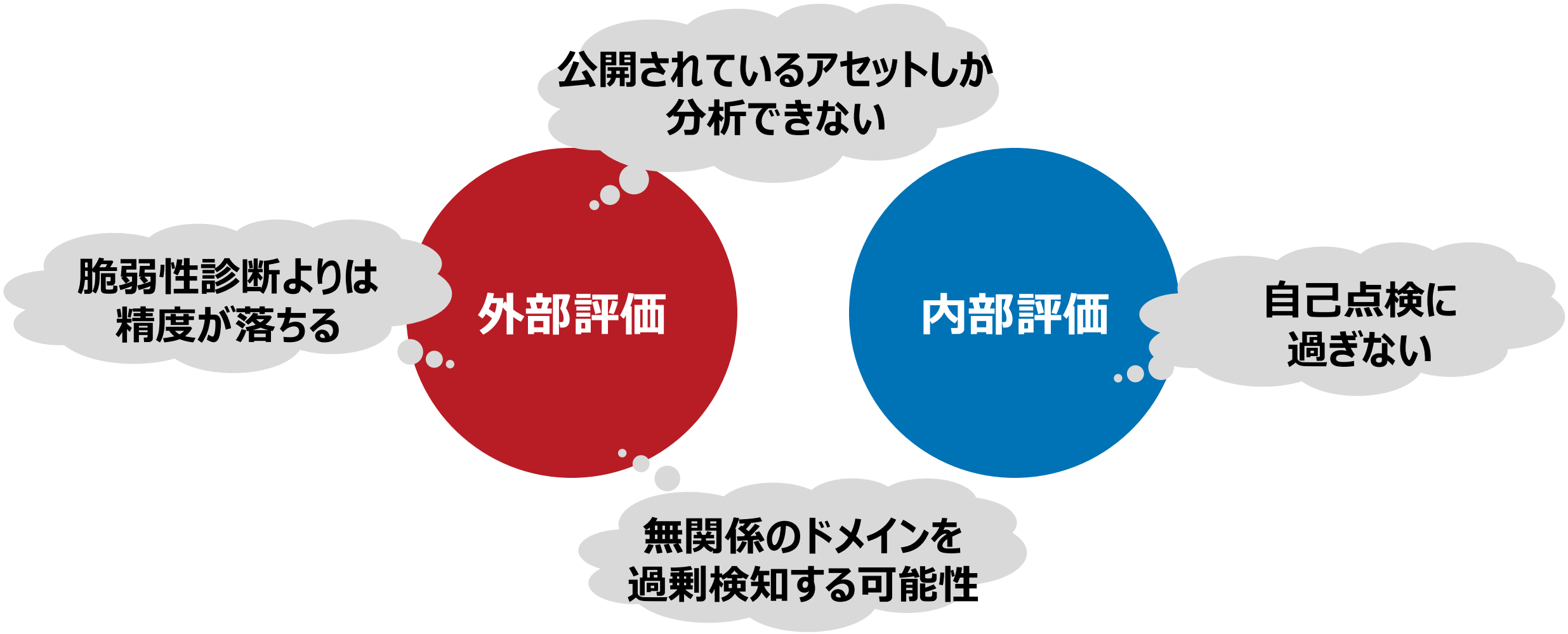


セキュリティ評価ツールのデータの使い方

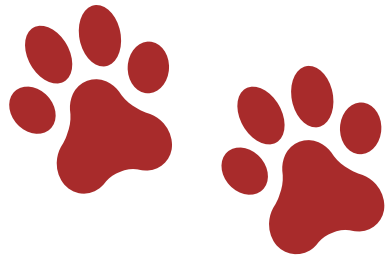
関係者に
フィードバック

改善の
サポート

セキュリティ評価ツールの限界

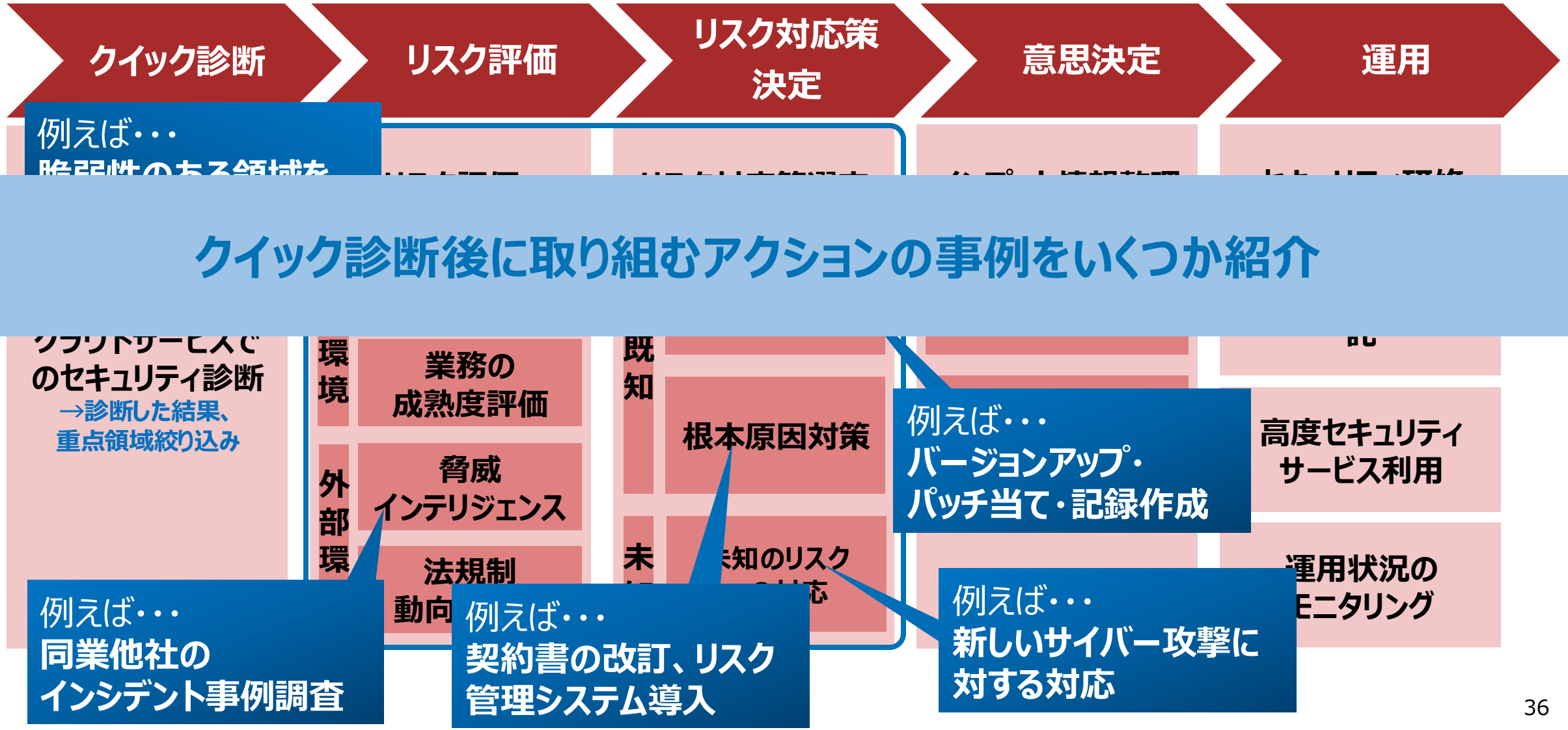


データを取得するのは、最初の一歩に過ぎない



データをどう評価するか？
どのような対応策を講じるか？
がより重要

クイック診断を手がかりに
サプライヤとともに、必要な対策の強化・より深い分析の実施を



業務の成熟度評価

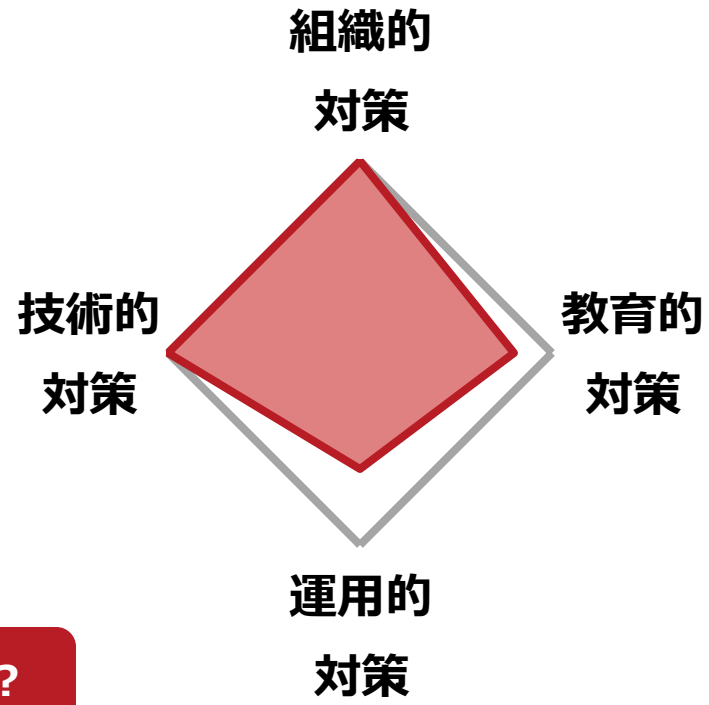
クイック診断や脆弱性診断のツールだけでは評価できない組織・業務プロセスのリスク診断

- **ISO27001**
- **NIST**
  Cyber Security Framework
- **IPA**
  情報セキュリティ対策ベンチマーク
- **業界ガイドライン**
  サイバーセキュリティガイドライン
- **リスクアセスメント**
  簡易セキュリティアセスメント

成熟度評価チェックリスト

チェックリストの内容は、様々なセキュリティ規則やガイドラインから選択もしくは自社で作成

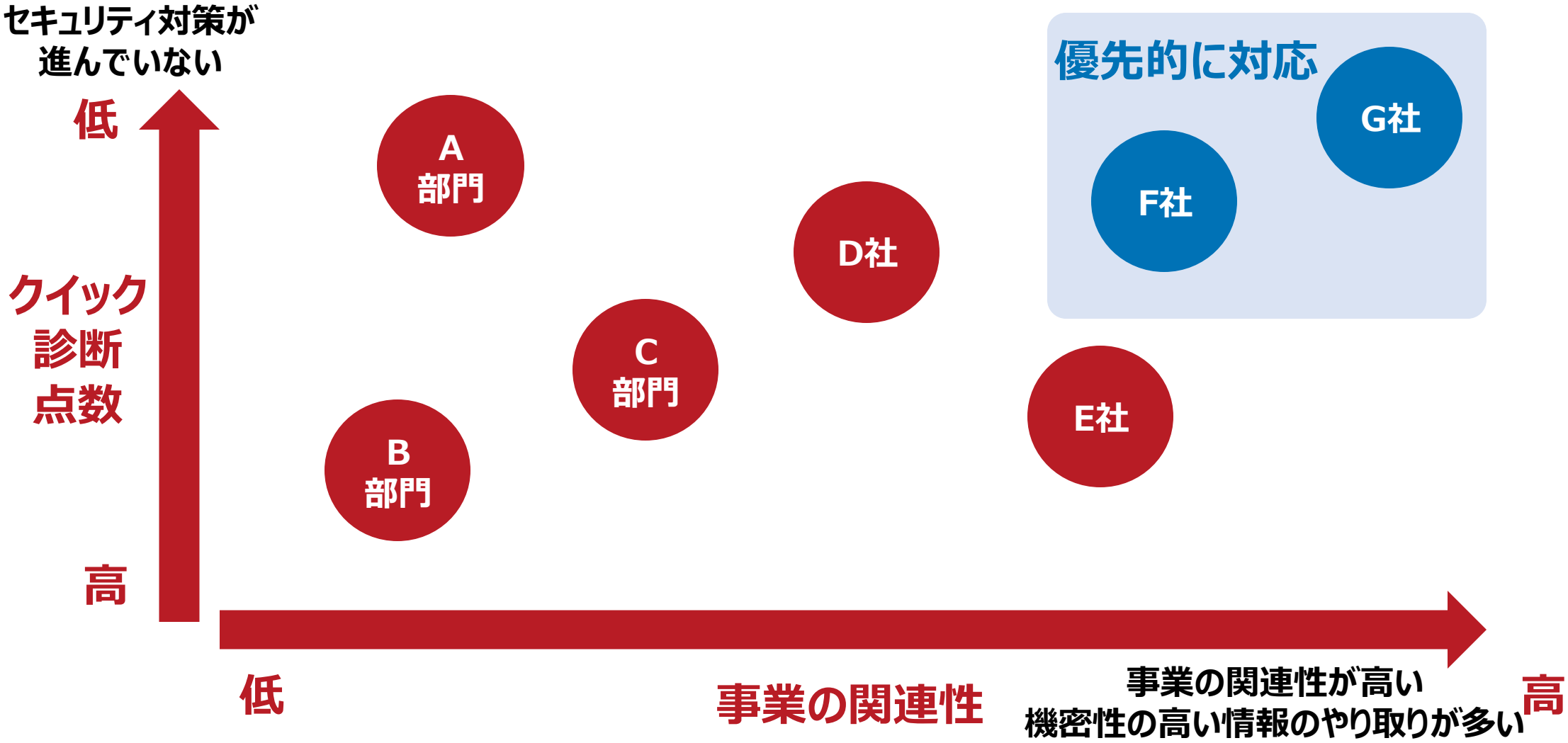
- 情報資産の棚卸を各部門ごとで定期的に実施していますか？
- システムの特権アカウントをどのように管理していますか？
- セキュリティ予算はどのようなプロセスで承認されていますか？



規制・ガイドライン調査 → 成熟度（セキュリティリスク）評価チェックリストの作成 → サイバーリスク診断

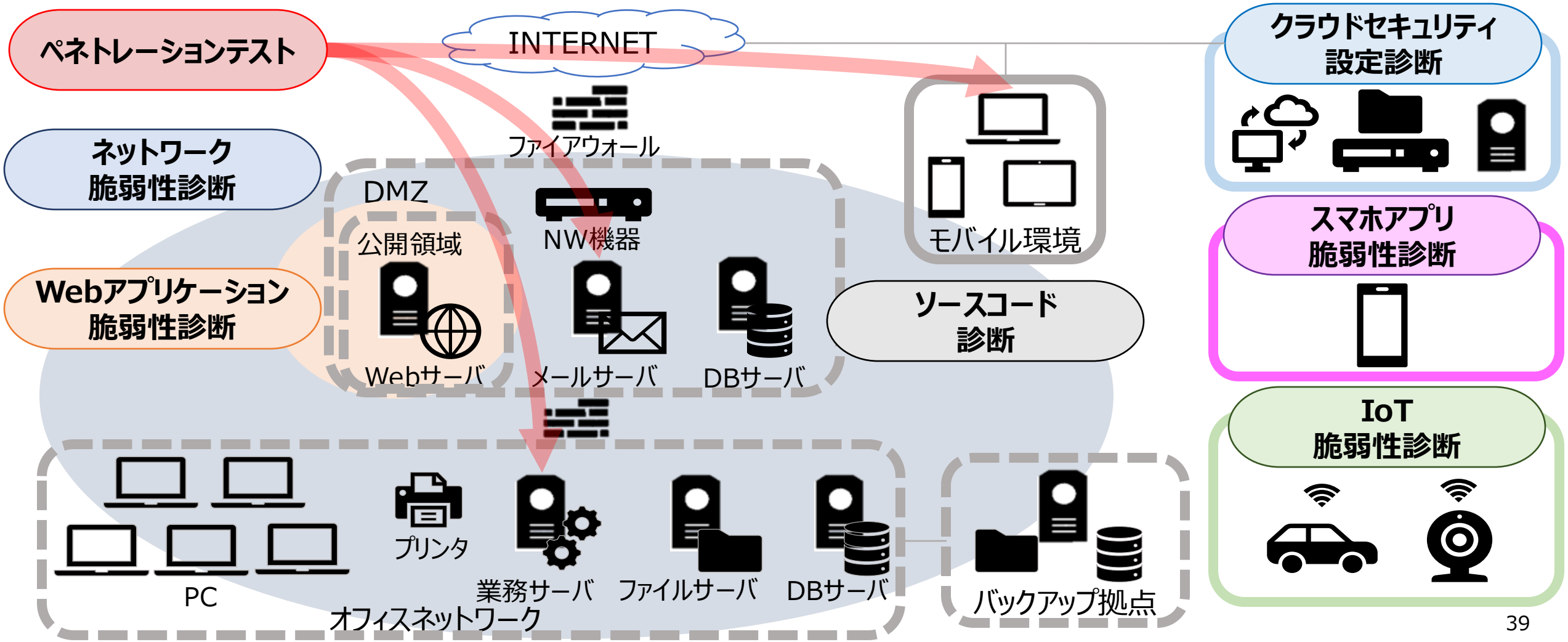
クイック診断

クイック診断で優先度の高いサプライヤーを把握



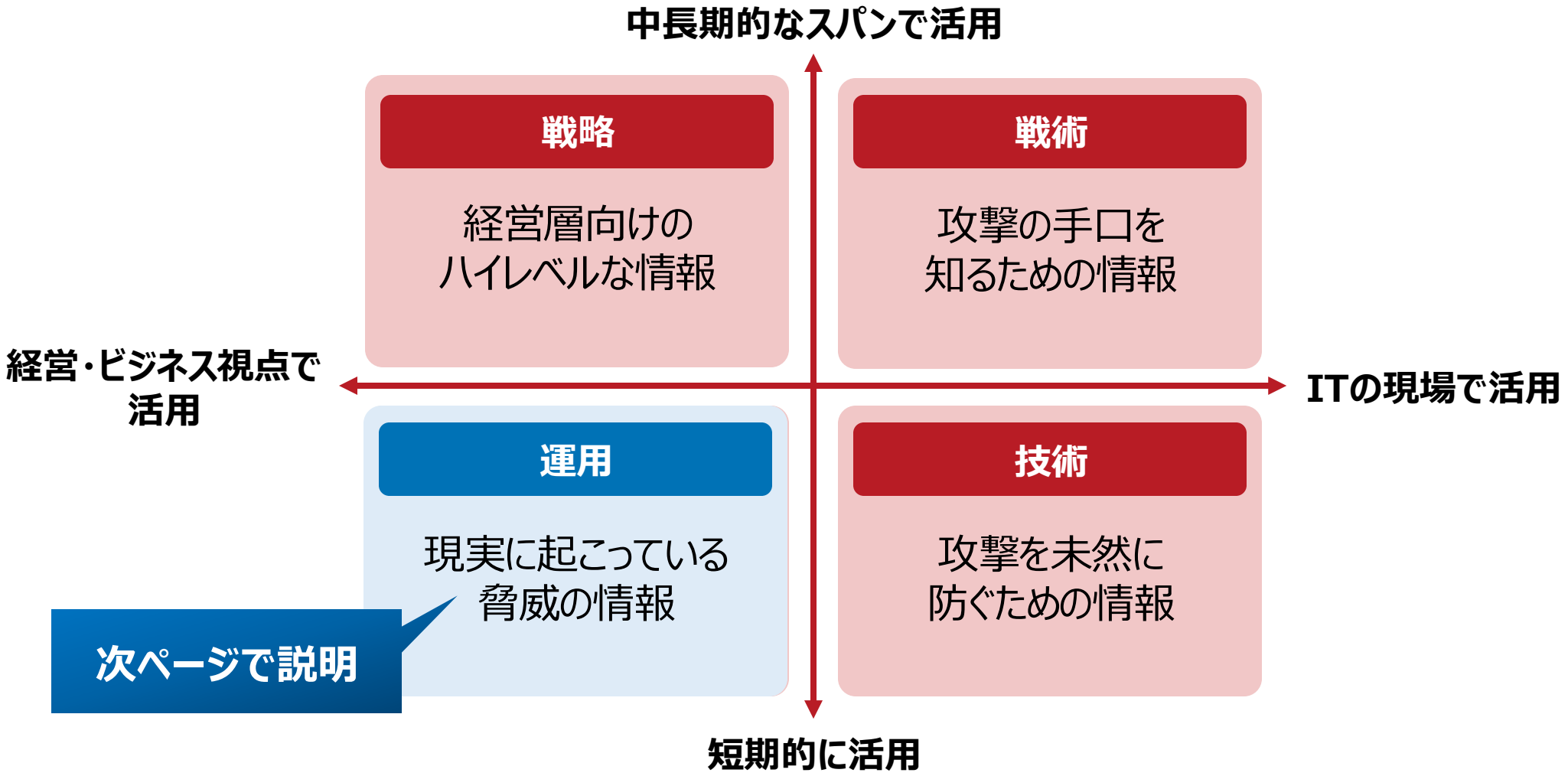
脆弱性診断

優先度の高いサプライヤーに対して、何の脆弱性診断(もしくはペネトレーションテストも対応)をするのか検討・決定



脅威
インテリ
ジェンス

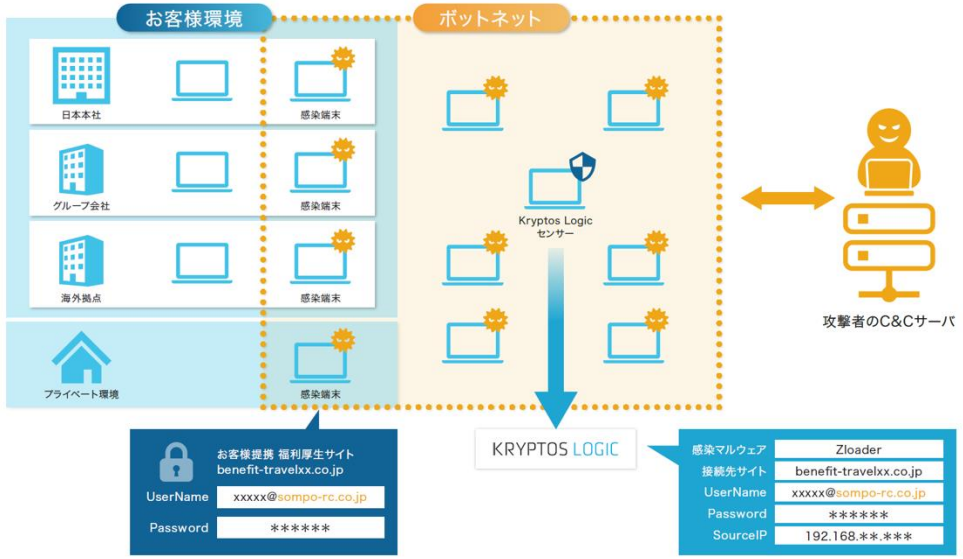
脅威の発生や検知に役立てるための攻撃者の意図・能力・設備などに関する情報を収集

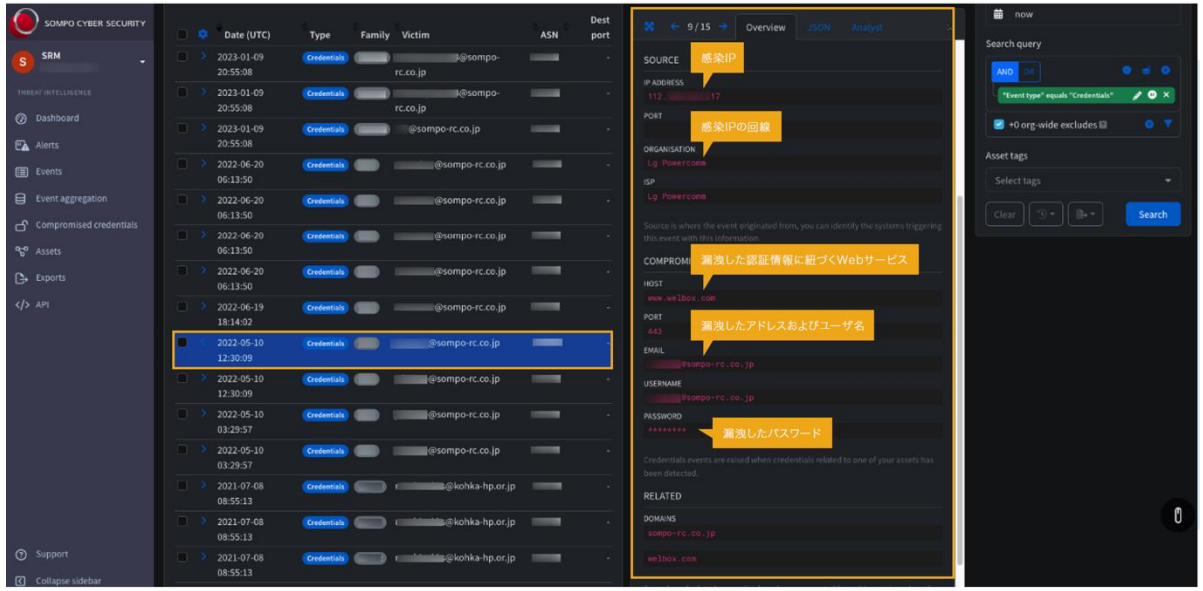


脅威インテリジェンス

例えば…ダークウェブ上での従業員のEmail・認証情報の流出を検知

クレデンシャルスタッフィング攻撃の検知・防御





従業員がプライベートでも会社のEmailアドレスを使用し
認証情報を使いまわしている場合に、
プライベート端末のマルウェア感染を契機として、
業務環境への侵入を試みられる可能性がある。

ダークウェブ上の情報から流出を検知して、
脅威情報を通知。
認証情報の変更や、
感染端末の再インストールなどを実施。

止血対策

業務の成熟度評価・脆弱性診断の結果、緊急性の高い指摘事項は、サプライヤに対応を促す

カテゴリ	発見された指摘事項・脆弱性（一例）	具体的な対策（一例）
アクセス権設定が適切ではない	・退職した社員のアクセス権が残っている（クラウドなど） ・社員全員が機密情報にアクセスできるようになっている ・システム運用者がAdmin権限を他者に共有している	・アクセス権の削除 ・ファイルごとのアクセス権の設定 ・Admin権限のモニタリング導入
パスワード管理に不備がある	・文字・数字・記号等を組み合わせでなく8文字以内 ・誕生日・配偶者の名前などをパスワードに利用している ・間違ったパスワード推測が多発してもロックアウトされない	・パスワードポリシー整備 ・ユーザーへの教育 ・アカウントロックアウトを設定
システムの更新ができていない	・OSのアップデートがされていない ・サポート切れのOSをネットワークに繋げて使っている ・最新のセキュリティパッチが当てられていない	・バージョンアップ ・ネットワークからの切り離し ・セキュリティパッチの適用

根本
原因対策

リスク評価した結果の根本原因対策（一例）
サプライヤーとの契約書の改訂

サプライヤーに対する セキュリティ要求事項改訂	自社のサイバーセキュリティ基準の改訂内容に基づき、 **各サプライヤーが遵守するセキュリティ要求事項を洗い出しし、 契約書に追加する項目を策定**する。
サプライヤーに 契約書の改訂調整・通知	各サプライヤーに契約書を改訂すること通知するために、 IT部門、事業部門、調達部門に連携・通知をし、 **サプライヤーと合意する対応ステップを調整**する。
契約締結	新しいセキュリティ条項を盛り込んだ契約書を **サプライヤーと締結**する。
サプライヤーの 定期セキュリティモニタリング	サプライヤーに対して **定期的なセキュリティモニタリング(自己点検・監査)を実施**し、 契約書に盛り込んだセキュリティ条項が順守されているかレビューする。

根本
原因対策

サプライヤとの契約内容改訂（重要な条項例）

①サイバーセキュリティ対策を講じさせる条項

- 取引先がサイバー攻撃を受けた場合を想定した条項として、
  取引先に一定のセキュリティ対策を講じることや一定のセキュリティ水準を確保することを義務づける条項。
- 取引先に過度なサイバーセキュリティ対策を要求することは、
  独占禁止法や下請法の問題にもなりうるため、
  取引先に生じるコストを適切に負担するなどの配慮が必要となる場合もある。

②報告義務を定める条項

- 自社の被害拡大防止を図るために、
  委託先がサイバー攻撃を受けた場合、若しくはその恐れがある場合
  ①適時に報告させる、②必要な調査や協力をさせる条項を設けることが望ましい。

③付保(ふほ)を義務付ける条項

- 取引先の信用不安の担保として、**契約実務上保険への加入（付保）を義務付ける条項**が存在する。
  (サイバーセキュリティでは民間保険会社によるサイバー保険が普及している)

未知のリスクへの対応

新たな事業領域や新たな国・地域に展開する際は新たなリスクの把握が必要

（一例）新たに海外進出を行ったA社の事例

A社：医療データを収集・解析するIT企業
欧州、アメリカ、東南アジアにビジネスを拡大。

新しい国に参入する場合は、
国によって法規制や商習慣が異なるため、
異なるセキュリティリスクが発生。

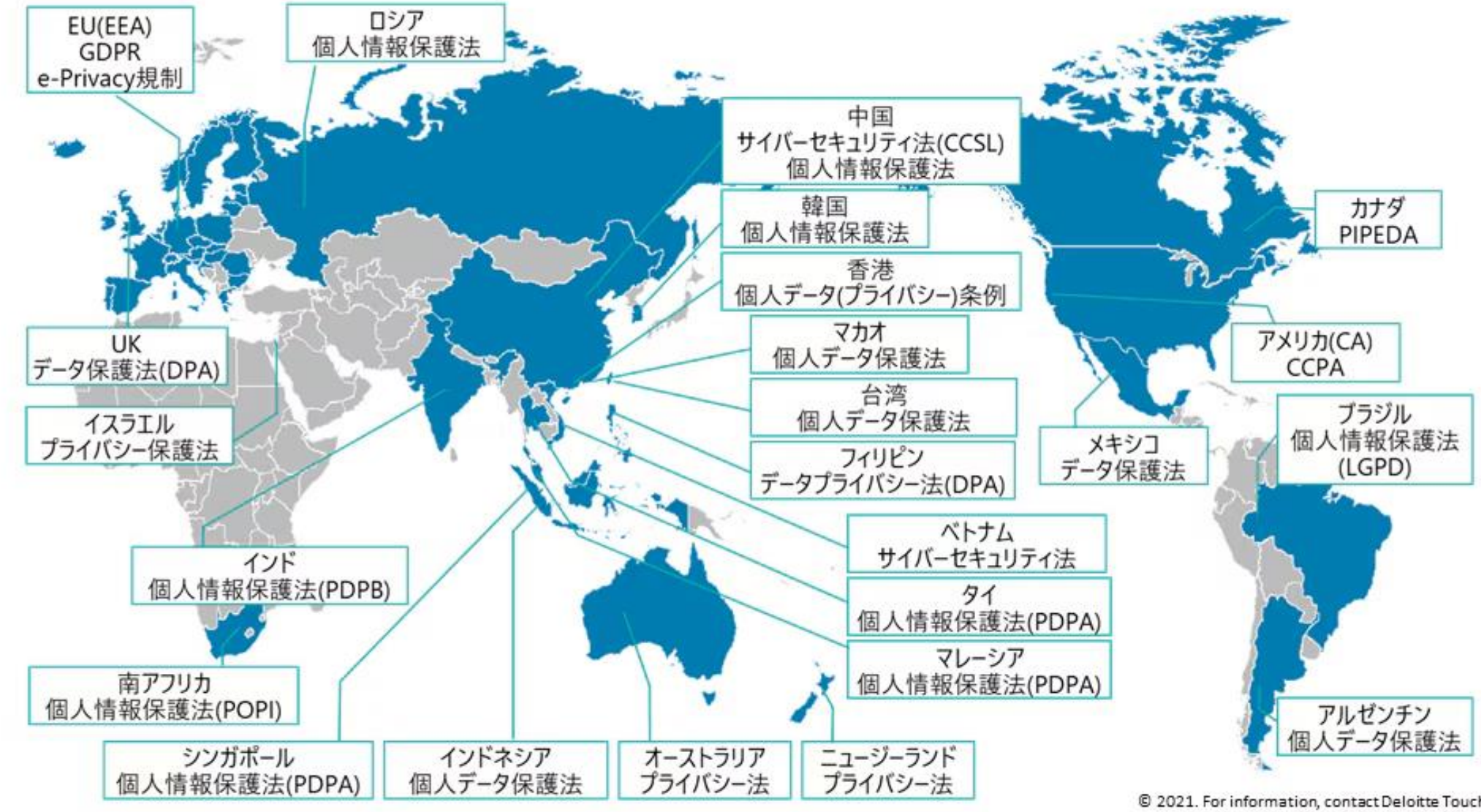
海外進出が初めてかつ
新しい医療サービスのため、
各国の法規制・業界団体に
具体的な取り扱いの情報がない。

各国のサイバーセキュリティ・個人情報の法規制から
医療データの授受に抵触する条項を整理し、
自社なりに解釈をして、
各国ごとに情報セキュリティ手引書を制定。

制定した手引書は
各国のサイバーセキュリティに強い
法律事務所のレビューも実施。
自社で制定することで、効率的なオペレーションも維持。

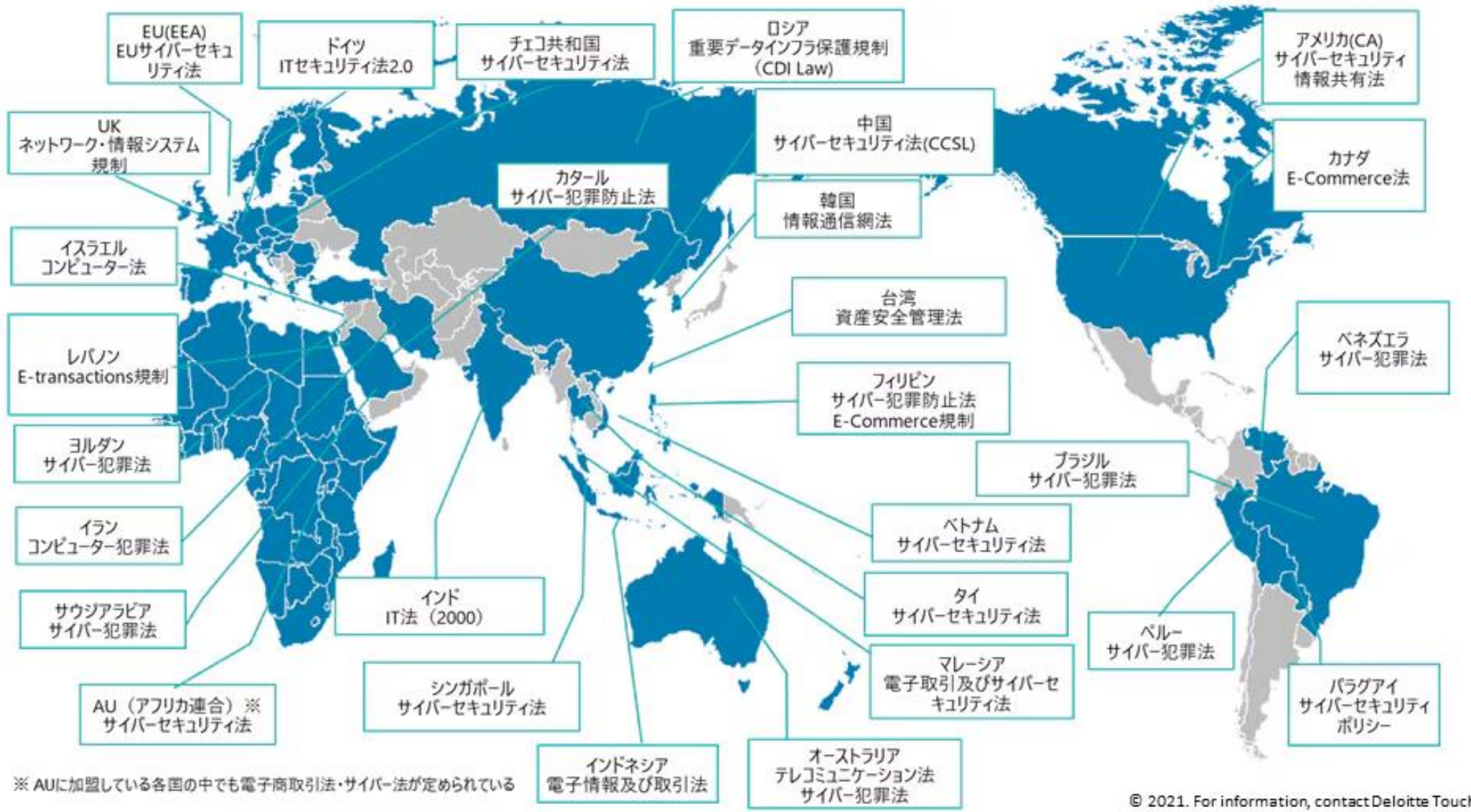
世界における個人情報保護規制の動向

※図には、本資料作成の時点(2020年12月)で、まだ法案であるものも含まれます。



世界におけるサイバーセキュリティ規制の制定・改訂状況

※図には、本資料作成の時点(2020年12月)で、まだ法案であるものも含まれます。



※ AUに加盟している各国の中でも電子商取引法・サイバー法が定められている

サイバーセキュリティ先進地域の状況

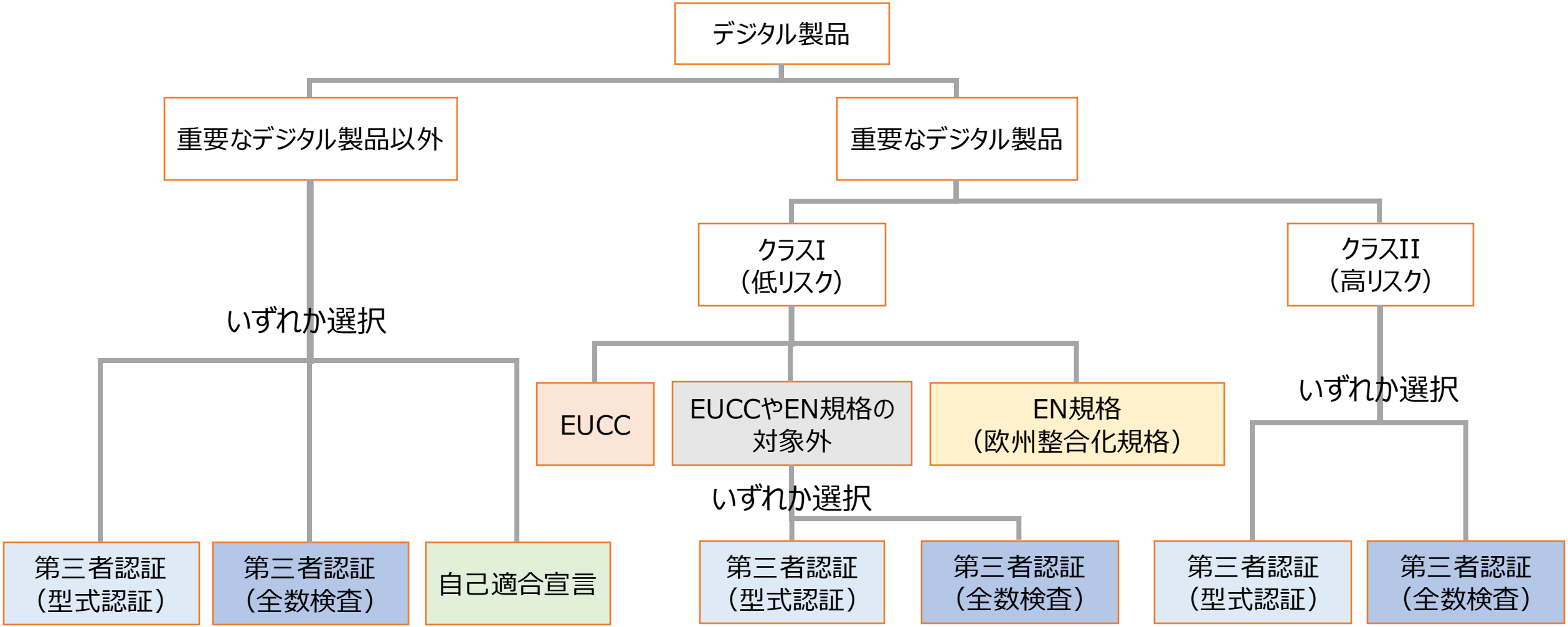
MASON consulting

国や州	関連法令
ドイツ	• German Bundesdatenschutzgesetz (BDSG)：ドイツ連邦データ保護法 • General Data Protection Regulation (GDPR)：EU一般データ保護規則 • LOI n° 2018-133：EU NIS指令の国内実施法
ポーランド	• General Data Protection Regulation (GDPR)：EU一般データ保護規則 • LOI n° 2018-133：EU NIS指令の国内実施法 • Urząd Ochrony Danych Osobowych（UODO）：ポーランドのデータ保護当局の規則
フランス	• General Data Protection Regulation (GDPR)：EU一般データ保護規則 • LOI n° 2018-133：EU NIS指令の国内実施法
イギリス	• UK General Data Protection Regulation (UK GDPR)：英国一般データ保護規則 • DPA2018：データ保護法
カリフォルニア州（アメリカ）	• California Consumer Privacy Act (CCPA)：カリフォルニア消費者プライバシー法 • California Privacy Rights Act (CPRA)：カリフォルニア州プライバシー権法
テキサス州（アメリカ）	• Texas Data Privacy and Security Act (TDPSA)：テキサス州データ・プライバシーおよびセキュリティ法 • Data Breach Notification law：個人情報漏洩時に対象者に通知する義務を課す法律
ネバダ州（アメリカ）	• Senate Bill 220 (SB220)：ネバダ州個人データ保護法修正 • Data Breach Notification law：個人情報漏洩時に対象者に通知する義務を課す法律
日本	• Act on Protection of Personal Information (APPI)：個人情報保護法 • サイバーセキュリティ基本法

欧米の最新サイバーセキュリティ・個人情報保護法・規制の動向

EU Cyber Resilience Act (CRA)-欧州サイバーレジリエンス法

「**デジタルの要素を持つ製品**」のサイバーセキュリティの欠陥からユーザー・消費者を守ることを目的としており、**違反した企業には巨額の罰金が科される**ことがある。



適合性評価方法

欧州サイバーレジリエンス法におけるデジタルの要素を持つ製品とは、何か？

「**デジタルの要素を持つ製品**」の範囲は、幅広い。『印刷事業を核に、グループのエンターテインメント及びアミューズメント事業を支援するとともに様々なサービスを展開』されている貴社でも関わる部分が多い。

対象製品区分	重要なデジタル製品以外の製品	重要なデジタル製品 クラスI（低リスク）	重要なデジタル製品 クラスII（高リスク）
定義	重要区分に入らないデジタル製品	• 重要ではあるが、リスクが低い	• 管理者権限を持つ • 広範囲に影響を及ぼす • 個人データなど機密性が高い
例	• 一般向けアプリケーションソフト • スマートスピーカー • ゲーム機器 など	• 産業用以外のネットワーク機器 • マルウェア検知ソフト • リモートアクセスソフト • パスワードマネージャ など	• サーバ、デスクトップ、モバイル機器などのOS • 産業用ネットワーク機器 • 公開鍵インフラ・デジタル証明書発行製品 • 産業用ファイアウォール、検知システム • EU「NIS2 指令」（重要エンティティ）該当の産業用IoT製品 など

Network and Information Systems Directive (NIS)2-NIS2指令

EU域内において加盟国によって求めるセキュリティ対策のレベル感が異なると、
一部の加盟国がサイバー脅威に対して脆弱になり、EU全体に波及する可能性がある。
そこで、**加盟国間の大きなセキュリティ対策の相違を解消する**ことを目的に、
NIS指令が廃止され、改正版として新たにNIS2指令が制定された。

NIS指令とNIS2指令の適用範囲の違い

NIS2指令で貴社に関わりそうな領域

EU域内において加盟国によって求めるセキュリティ対策のレベル感が異なると、
一部の加盟国がサイバー脅威に対して脆弱になり、EU全体に波及する可能性がある。
そこで、**加盟国間の大きなセキュリティ対策の相違を解消する**ことを目的に、
NIS指令が廃止され、改正版として新たにNIS2指令が制定された。

NIS指令とNIS2指令の適用範囲の違い

AI-ACT

EU域内で提供される**AIシステムの安全性や信頼性と基本的人権の尊重を確保**すべく、
域内で一律に適用されるAI規制枠組みを規定する。

サブリミナル技術や操作的・欺瞞的な技術を用いて人の行動を歪め、人が通常は行わないような、重大な損害をもたらす決定を行わせるAIシステム

許容できないリスク

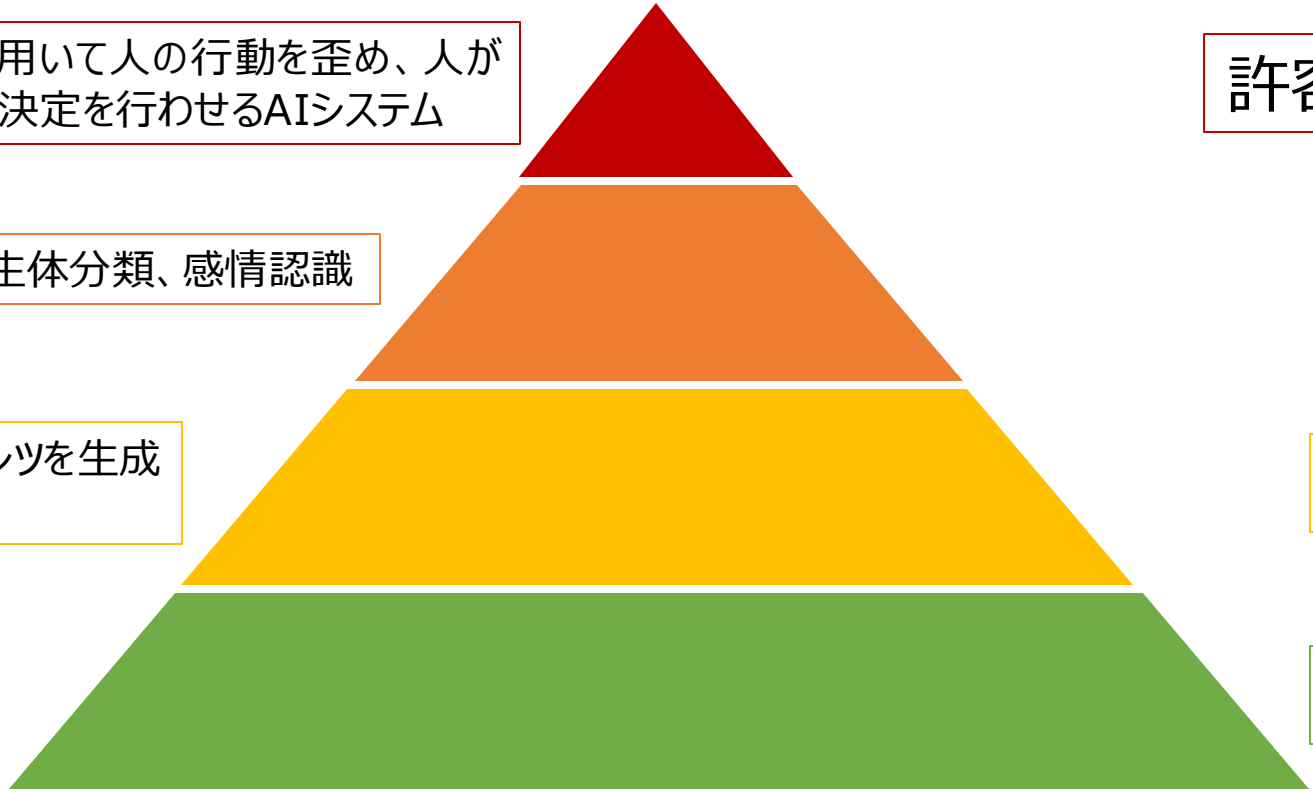
自然人の遠隔生体識別、機微情報に基づく生体分類、感情認識

高リスク

人工音声、画像、動画、テキストなどのコンテンツを生成するAIシステム

限定リスク

最小リスク



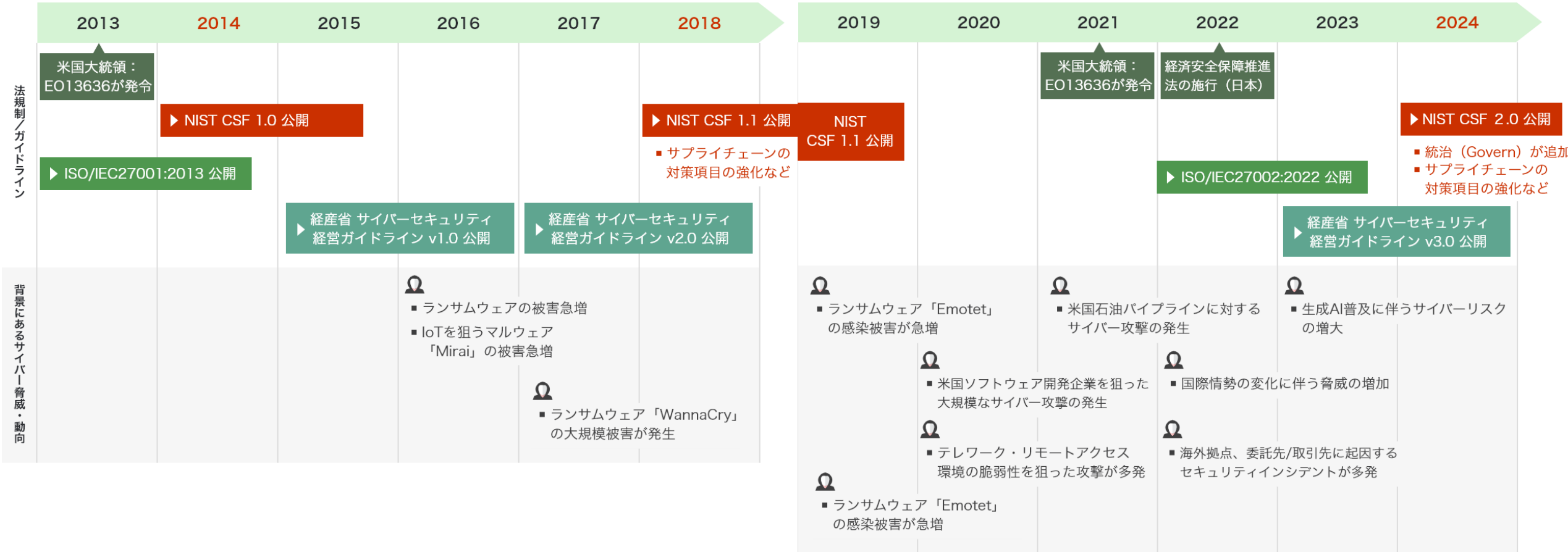
汎用目的型人工知能 (GPAI)

NIS指令とNIS2指令の適用範囲の違い

NIST CSF 2.0

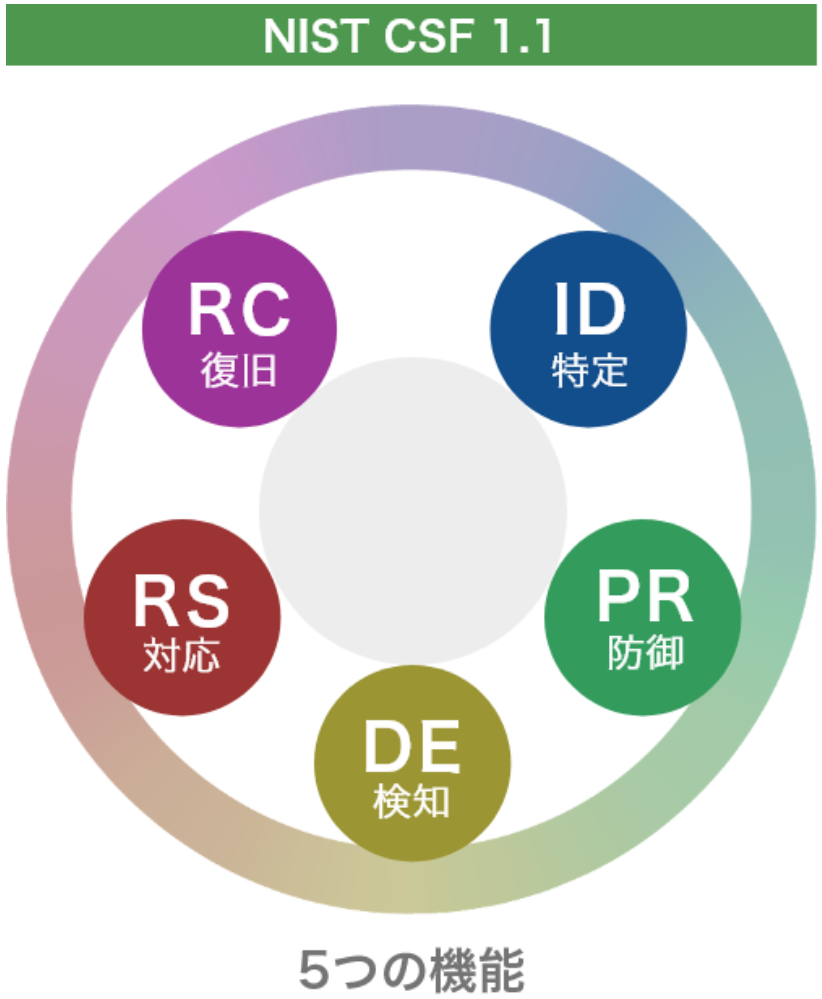
MASON consulting

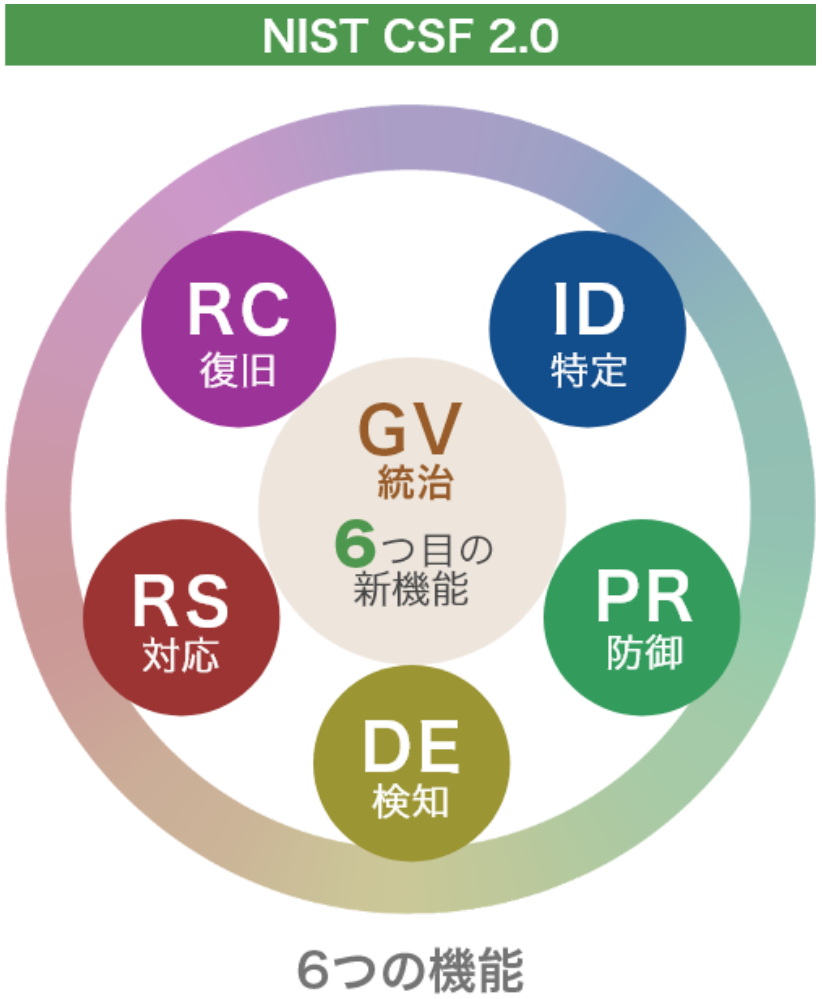
重要インフラシステムの複雑化と持続性の向上を巧みに利用し、**国家の安全保障、経済及び市民の安全と健康を脅かすリスクへの対処を強化・改善することを目的**として策定された。



NIST CSF 2.0

NIST CSF 2.0では、サプライチェーンリスクマネジメントの強化もなされており、
既存のNIST CSF 1.1の内容を踏襲しつつも、**管理要件が新設**されている。





国内の活用事例

より深い分析
弱点に応じた対応

公開IT資産の評価
サプライヤーと協議・セキュリティ教育実施

導入事例 CASE STUDY

Panorays

横浜銀行

POINT
- 既存の調査票＋外部評価の二重構造
- 調査票をプラットフォーム上で一元管理
- 自社とグループ会社＋委託先と取引先の評価が可能

求められるデジタル化への対応
～柔軟に、スピーディに、かつ安全に～

オンラインバンキングやオンライン決済、スマホ決済、私たちの暮らしがデジタル化するにつれて、銀行に求められる役割、銀行のあるべき姿というのも劇的に様変わりしています。こうした環境の変化に順応し、銀行として成長を続けるためには、外部との協力、連携が不可欠です。求める技術を開発している企業を買収したり、求める事業を既に展開している企業と業務提携したり、また、専門性を生かした事業を展開する企業に業務の一部を委託したり、いわゆるサードパーティと呼ばれるビジネスパートナーの数は気が付けば数千を超えている事業者も少なくないのが現状です。

そのサードパーティに開発を委託したり、個人情報などの機密データを共有したりすることによって利便性は高まりますが、同時に、今までになかったリスクも生ま

金融業界全体のサイバーセキュリティの底上げに

ICT 推進部 セキュリティ統括室 ビジネスリーダー
吉嶋 正和氏

ICT 推進部 セキュリティ統括室長
砂田 浩行氏

ICT 推進部 セキュリティ統括室 ビジネスアシスタントリーダー
伏見 亮大氏

■ 委託先などのサプライチェーン管理の課題

【砂田氏】:
二つ目は資本関係のない委託先などのサプライチェーン管理という非常に難しい課題があります。例えば、システム開発や個人情報の委託先であれば、従来通りの情報セキュリティの観点でこういうものに準拠してくださいというチェックリストがあるので、そこは問題ないのですが、一部の業務委託先などに関しては、今まであまり明確にポリシーがありませんでした。ある一部の業務を委託しているだけなのに、当行のセキュリティポリシーを適用させるとなるとハードルがかなり高いのが現状です。多くの銀行がシステム開発を委託している大手ベンダーが、各銀行のポリシーを把握し全ての要件を満たすというのは大変な手間がかかります。

東京オリンピックがあった年に、サイバーインテリジェンスサービスのトライアルを実施しましたが、重要なシステムを委託しているベンダーで、かなりの数の脆弱性が検出されました。誰もが知るような大手ベンダーでさえ、そういった状況なので、一顧客として、全部の脆弱性に対して修正してください、というのは、かなり難しい、というのが現実にどの企業も直面している課題だと思います。

あとは、委託を開始する前の審査もありまして、上述のチェックリストがありますが、アタックサーフェイスをスキャンして、脆弱性の有無やリスク度合いを評価後、取引の可否を判断するような審査は行っていません。日本の商慣習にそういう文化がまだ根づいていないということもあります。

下請法の問題もあり、立場の優位性を利用して取引を停止するとなると、別の問題になる可能性があり、非常に神経を使います。

【砂田氏】:
もう一歩踏み込みたいのは、複数の金融機関で共同利用するというコンセプトです。

内部評価(アンケート)に関して言えば、例えば複数の銀行でそれぞれ数百~千社の委託先を抱えているとして、ものすごい数のやり取りが発生しているはずです。そこの事務にかかる時間と負担を軽減できないか、と。アンケートが統一されれば、入力する側の負担も軽減できます。複数の銀行に同じ内容を返していたのが、1回記入すれば共有してもらえる、そういう使い方をすることによって、双方にメリットが出るというのはすごく我々がこれから期待している使い方です。

外部評価に関しては、金融機関の間で委託先のリスク評価を共有したい、という将来的な構想があります。点数で委託先を切るとか、そういうことではなく、単独で委託先に対して「改善してください」と訴えるよりも、複数の銀行が口を揃えて依頼をかけることで改善の方向に動く可能性も高くなると思っています。結果として金融業界のサプライチェーン全体のセキュリティの底上げ効果に繋がると思っています。強制的ではなく、可視化することで、自発的に取り組む雰囲気を作り、先程お話したサプライチェーン管理の課題を解消していくことで、金融業界全体のより安全な経営に繋がるのではないか、という期待があります。

【伏見氏】:
Panoraysの導入で課題だったのが、アンケートの取り込みです。今までエクセルで管理していたアンケートを取り込もうとしていますが、アンケートの内容が適切なのかということは、今後、Panoraysを使用していく中で考えないといけないと思っています。アンケート機能という観点でも、SaaSならではの、適切な質問の仕方などもあるはずで、その辺りのノウハウを頂いて、我々の中でのアンケートの実施方法を改善していく必要があると考えています。

どういった観点を質問すべきか、聞き方も、より統計を取りやすくする工夫が必要かと。他行に展開するとなると、共通のアンケートを作ることになると思うのですが、単純にエクセルの各行のアンケートを統合して、プラットフォームにアップロードすればいいという考え方だと、多分スケールしていかないですし、単純に項目が増えていくだけで、質問内容自体、委託先の適切な評価に繋がるものなのか、精査されないまま増えていってしまうと、あまり意味が無い使い方になってしまいます。こういうような質問形式でやっていくべきという指標は、今後Panorays社の方からノウハウ等頂ければと思っています。

Panoraysでは、PCI DSSなどの各種基準に即した質問票が用意されています。我々もそういった〇〇に準拠した質問票というものを作る必要があると考えています。Panoraysのようなツールを使ったサプライチェーンの管理の仕方が、今後、銀行業界に広がっていくとなると、この質問票の項目自体が業界スタンダードになっていくと思うので、そこも含めて、内容のところへの精査、検討というのは今後しっかりやっていきたいと思っています。

【吉嶋氏】:
ちょっと前にサプライチェーンリスクとかサードパーティリスクマネジメントとは少し系統は違いますが、NTTドコモ口座事件というのがありました。まさにあの事件に象徴されるようなFinTech事業者が事故を起こすと、システムで繋がっている銀行も被害を受けるというリスクがあります。似たような事件はまだ起きていますが、各銀行が求める質問票に回答するのは非常に大変だとFinTech事業者側が仰っているのを伺ったことがあります。1、2年前に業界団体のイニシアチブで質問項目を統一しましょう、という取り組みがあり、結果、審査プロセスがスムーズになったということもありました。業界としてFinTech事業者に限らず、委託先に対してはチェック項目を統一化するようなことを今後は進めていく必要があります。イニシアチブをとる組織がいるというのが条件にはなりますが、そういった取り組みにPanoraysが活用できる可能性は十分にあると考えています。

海外の活用事例

チームスポーツで対応 ｜購買部門～IT部門までの部門横断

About the interview partner

Michael Deckert is an expert in cyber security in the supply chain at Siemens. Since 2019, he has headed the Taskforce for Responsibility in the Digital Supply Chain at the Charter of Trust.

About the series

In the Charter of Trust in Action series, we shed light on how the taskforces and partners of the initiative tackle innovation and promote cybersecurity. Be sure to check out our other interviews as well:

SIEMENS

How does collaboration contribute to a secure supply chain?

Cybersecurity is a team sport: internally, the various specialist departments from purchasing to IT must work together to identify risks at an early stage. But we also need collaboration externally. The business world is becoming increasingly interconnected; we at Siemens alone have thousands of suppliers, who in turn have thousands of suppliers themselves. If we now tried to keep an eye on the cyber security of all the supply chains all year round on our own, we would reach our breaking point. Only by agreeing on common standards and processes with our partners can we make it work.

How is the Charter of Trust working to protect supply chains?

When we first started talking about supply chain cybersecurity at the Charter of Trust, we encountered two issues: one was the high volume and complexity of suppliers, and the other was a lack of appropriate tools and approaches. Depending on the country, industry and company policies, suppliers use different standards, which make mutual data exchange a challenge.

サプライチェーンセキュリティの活動は
社内・社外のステークホルダーが多い活動のため、
トップマネジメントの関与が成功要因に

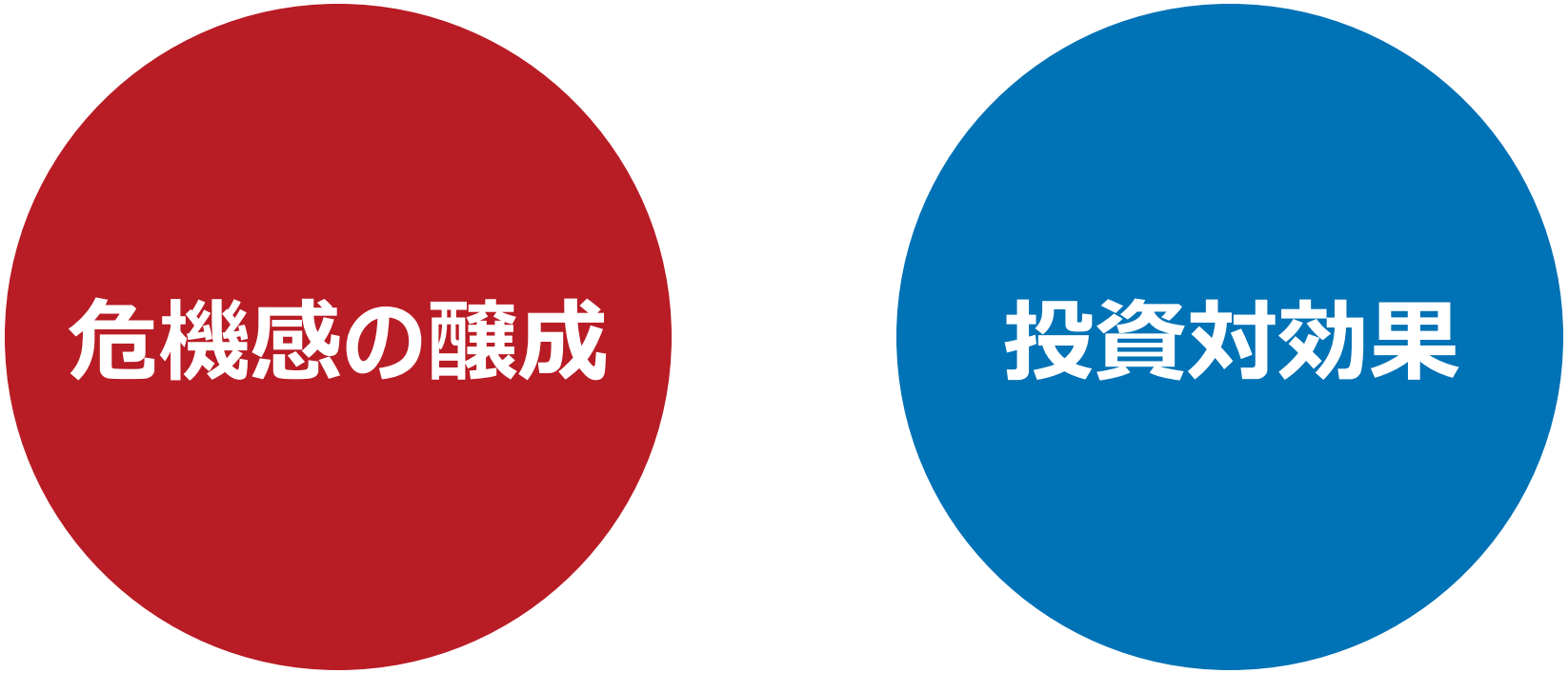
サプライチェーンセキュリティに取り組む前提として・・・
経営陣にセキュリティ投資の必要性を
認識してもらうことが不可欠

他の事業リスクは
経営会議の議題になっているのに…
サイバーセキュリティリスクは
何故取り扱われないのか？

サイバーセキュリティリスクを認識し
意思決定するための
情報が足りない…

セキュリティ投資の意思決定のために

経営者が求める2つの情報



危機感の醸成

自社がリスクに晒されていることを
正しく認識できる情報

例えば・・・
・ダークウェブへの情報流出事例
・ホワイトハッカーの攻撃による脆弱性の把握
・同業他社のインシデント事例

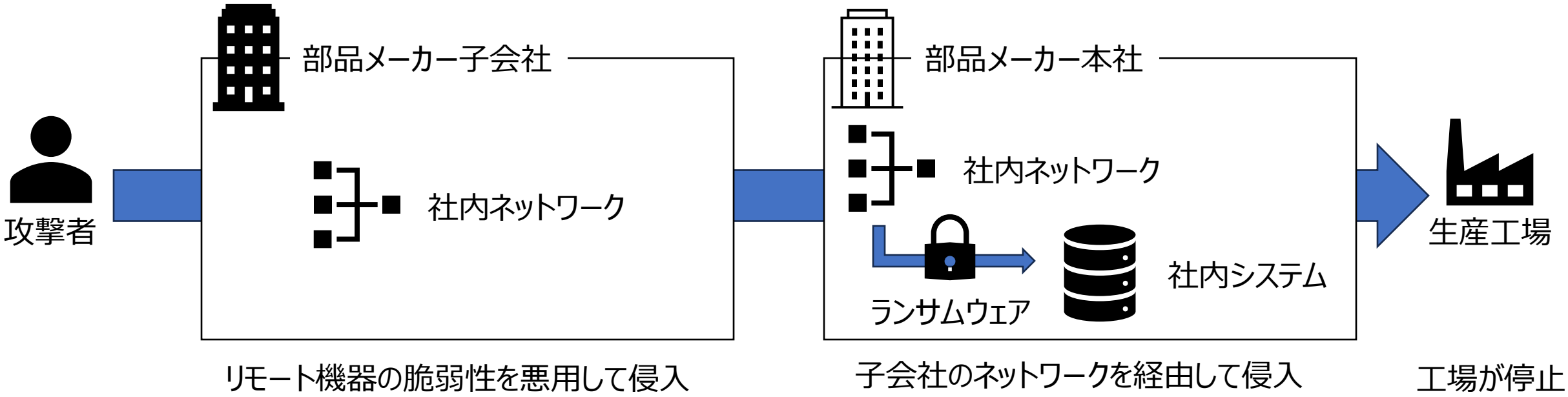
Y社（自動車保険会社）から漏洩した
データベース50万件を販売するという、ダークウェブ上の実際の投稿

Emailアドレス・顧客のフルネーム・病歴・保険契約の詳細などを含むデータを販売

ダークウェブマーケットBreachに投稿されたデータベース販売投稿　出典：Cognyte Luminar
https://www.sompocybersecurity.com/column/column/insurance-group-japan-db-sale より

サイバー攻撃による事業停止リスク

サプライチェーン攻撃による操業停止の事例	
概要	• 2022年2月、取引先の部品メーカーでのシステム障害を受け、国内全工場（14拠点28ライン）の稼働を停止した。 • 部品メーカー子会社が利用していたリモート接続機器の脆弱性を悪用し、ネットワークに侵入、さらに部品メーカー本社のネットワークに侵入された。 • 結果、メールなどの社内システムなどが稼働できなくなったほか、部品発注・受注や納品データのやり取りをする基幹システムが停止。
影響	国内全工場が稼働停止したことで、約10,000台強の自動車の生産に影響、同年1月の月間生産台数の5%に相当すると言われている。



サイバー攻撃は、事業継続に直接的な影響を及ぼす。

大手サービス業のグループ会社で発生したランサムウェア感染と標的型メールのテスト結果

事故概要	20XX/XX/XX午前XX時頃、社内システムにランサムウェアLockBitが侵入。 社内の機器類への侵入と感染を継続、社内の複数のPCおよびサーバに感染し、ファイルを暗号化。 交渉を要求する文章がプリンタより大量に印刷される。
侵入原因	以前、社内PCに送り付けられたフィッシングメールをクリックしたことにより、社内システムに侵入。
情報の流出について	情報セキュリティ会社による情報の流出についてサーバログ、トラフィックなどを調査した結果、社内データが外部へ漏洩した痕跡は無く、情報の流出は確認され無かった。
行政機関への報告	11/XX　JIPDECおよび個人情報保護委員会に報告書を提出
損害状況	情報機器関連、復旧作業費用、調査関連費用など **合計約1,500万円の損害**

対象者	実施者	対象者数	開封者数	開封率	開封報告者数	開封報告率
A社 （グループ会社）	大手サービス業グループ情報セキュリティ委員会	235 人	13 人	**5.5 %**	9 人	69.2 %
東商会員企業 （従業員 300 名以下）の経営者・従業員（公募）	東京商工会議所	811 人	99 名	**12.2 %**	N/A	N/A

未だに、標的型攻撃にかかる人は多い状況。

投資対効果

投資対効果を、他の事業リスクと横並びで比較できる情報

具体的には・・・

・**ROSI**(Return On Security Investment)の計算

$$\mathbf{ROSI} = \frac{\text{リスク削減額(想定損害額×発生確率)}}{\text{情報セキュリティ対策投資額}} \times 100\ (\%)$$

ROSI算出事例

$$\text{ROSI}：\frac{(33{,}500①\times 0.38②)}{3500③}\times 100\ (\%) = 364\%$$

① 想定損害額：33,500万円(他社事例参照)
損害額内訳：
- ✓シンクライアント化全PC: 12,000万円
- ✓多要素認証システム導入費用: 1,000万円
- ✓システム停止による損失(営業日数から算出): 20,000万円
- ✓データ復旧費用: 500万円

※レピュテーション被害は含まず

②ランサムウェアの発生確率：38%(Nikkei記事参照)

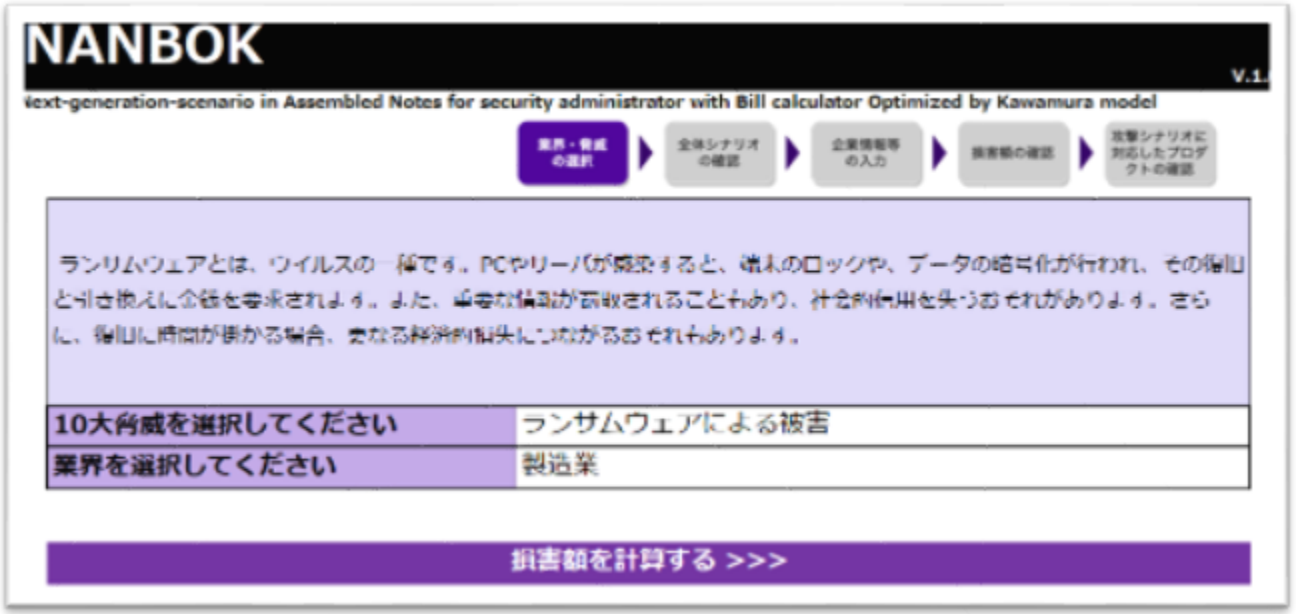
③セキュリティ投資額：3,500万円
セキュリティ投資額の内訳
- ✓脅威インテリジェンス 3,000万円
- ✓人的リソース追加： 500万円

レピュテーション被害を除いても、ROSIは364%
セキュリティ投資は高いリターンを生むため、経営層に報告

*:ランサムウェア被害調査　日本は「支払い渋りで減少」- 日本経済新聞 (nikkei.com) 2024/5/31

参考情報｜想定損害額の計算

IPAのWebサイトで、情報セキュリティ10大脅威に関わる事象が発生した場合の想定損害額の計算に役立てられる計算シート「NANBOK」が提供されている。

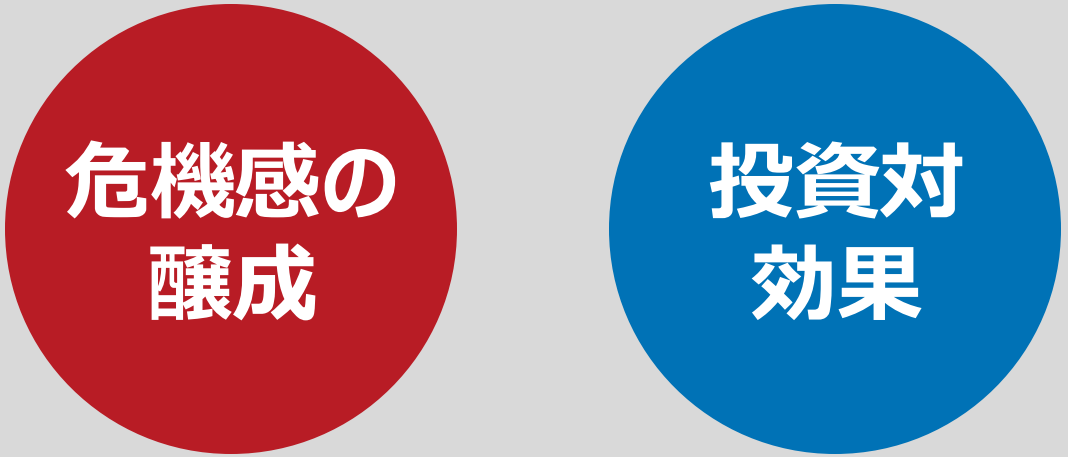


業界・対象となる脅威を選んで情報を入力すると計算される

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/visualization-costs.html

セキュリティ投資の意思決定のために

経営者が求める2つの情報



どちらも、技術面・経営面での両面で、専門的な知見が必要

技術的な情報をベースに
「経営の言語」でコミュニケーションを取る必要がある

サプライチェーンセキュリティ検討組織やWG

	組織名	開始年度	代表者	組織概要・目的	WG
	CSAJC (Cloud Security Alliance Japan Chapter)	2010年 6月	笹原英司 寺尾敏康	クラウド・コンピューティングのセキュリティを保証するベストプラクティスの使用を推進し、クラウド・コンピューティングを使用するにあたってあらゆるコンピューティング環境を安全にするための教育を提供するために設立。	①CCMWG ②ゼロトラストWG ③クラウドセキュリティWG ④CASBWG ⑤プライバシWG ⑥AIWG など13WGがある。
	CoT (Charter of Trust)	2018年 2月	Siemens AG	デジタルエコシステムを保護するために、国際的に調和されたサイバーセキュリティの標準と規範の開発、推進、使用の促進を図るために設立。	CoTの10の原則に基づく10つのTFで構成されている。Principle 2 はサプライチェーンセキュリティで18のベースライン要件を産学官へ普及活動をしている。
	Cybersecurity Tech Accord	2018年 4月	N/A	あらゆる場所のユーザと顧客を保護し、サイバー空間のセキュリティ、安定性、レジリエンスを向上させることを目的に設立。	N/A
	JNSA (特定非営利活動法人日本ネットワークセキュリティ協会)	2001年 5月	江崎浩	ネットワークセキュリティに携わる組織が結集してネットワーク・セキュリティの必要性を社会にアピールし、かつ、諸問題を解決していく場の構築を目的に設立。	①CISO支援WG ②中小企業支援施策WG ③JNSA-CERC など
	CISA (Cybersecurity and Infrastructure Security Agency)	2018年	Jen Easterly	国土安全保障省に設置されていた国家防護プログラム局を改組し、その責務を明確化し、独立性の高い組織とするために設立。	他の政府機関などとも連携し、ICT Supply Chain Risk Management Task Forceなど複数のWGの活動をおこなっている。

サプライチェーンセキュリティ検討組織やWG

	監督機関	組織名	開始年度	代表者	組織概要・目的	WG
SC3	IPA	SC3 (サプライチェーンセキュリティコンソーシアム)	2020年 11月	遠藤信博	産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進運動を進めていくことを目的に設立	①産業連携WG ・・SCS成熟度モデル検討SWG ・・工場セキュリティ共創SWG ②国際WG ③人材教育・育成WG
SiP	主導： CSTI 実施機関： NEDO	SIP (戦略的イノベーション創造プログラム)	2018年	議長： 内閣総理大臣	Society 5.0の実現に向け、様々なIoT機器を守り、社会全体の安全・安心を確立するため、IoTシステム・サービスおよび中小企業を含む大規模サプライチェーン全体を守ることができる「サイバー・フィジカル対策基盤」の開発と実証	①実証評価WG ②成果普及WG ③海外動向調査WG
JCIC Japan Cybersecurity Innovation Committee	N/A	JCIC (一般社団法人日本サイバーセキュリティ・イノベーション委員会)	2017年 11月	梶浦敏範	サイバーセキュリティに関する政策提言や研究活動を行うために設立	①政策研究WG ②人材育成WG ③今後のWG
経済産業省 Ministry of Economy, Trade and Industry	経済産業省	産業サイバーセキュリティ研究会	2017年 12月	座長： 村井純 (慶応義塾大学教授)	産業界が目指すべきサイバーセキュリティの方向性について、産業界を代表する経営者やインターネット時代を切り開いてきた有識者等から構成されるメンバーに、大所高所から議論いただくために設立	①制度・技術・標準化WG ②経営・人材・国際WG ③サイバーセキュリティビジネス化WG ④サイバー攻撃による被害に関する情報共有の促進に向けた検討会

サプライチェーンセキュリティガイドライン検討組織

	組織名	代表者	ガイドライン最新年度	ガイドライン目的・概要	ガイドライン
jama Japan Automobile Manufacturers Association 一般社団法人 日本自動車工業会	JAMA (一般社団法人自動車工業会)	片山正則	2024年8月	自動車メーカーやサプライチェーンを構成する各社に求められる自動車産業固有のサイバーセキュリティリスクを考慮した対策フレームワークや業界共通の自己評価基準を明示することで、自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進することを目的に策定。 自己評価結果の提出方法のシステム化に伴う入力項目追加と誤記修正を実施したセキュリティガイドラインが最新バージョンとなっている。	自動車産業サイバーセキュリティガイドライン
JAPIA Japan Auto Parts Industries Association	JAPIA (一般社団法人日本自動車部品工業会)	茅本隆司			
金融庁 Financial Services Agency	金融庁総合政策局リスク分析総括課ITサイバー・経済安全保障監理官室	齊藤剛	2024年10月	2024年10月4日に「主要行等向けの総合的な監督指針」等を一部改正し、新たに各監督指針・事務ガイドライン（以下、監督指針等）の別紙となる「金融分野におけるサイバーセキュリティに関するガイドライン（以下、本ガイドライン）」を金融機関等向けに公表。	金融分野におけるサイバーセキュリティに関するガイドライン
経済産業省 Ministry of Economy, Trade and Industry	経済産業省商務情報政策局サイバーセキュリティ課	武尾伸隆	2023年3月	独立行政法人情報処理推進機構（IPA）とともに、大企業及び中小企業（小規模事業者を除く）のうち、ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため、「サイバーセキュリティ経営ガイドライン」を策定。	サイバーセキュリティ経営ガイドライン

本日お伝えしたいこと

- サプライチェーンセキュリティ強化のため、
  まずは**評価サービスを使ってサプライヤーを「クイック診断」する**ことが望ましい。
- ただしクイック診断は万能ではないため、サプライヤと連携し、
  経営者主導で、必要なセキュリティ対策を追加で実施することが重要。
- 必要なセキュリティ対策の投資を意思決定するためには、
  投資対効果に基づいて経営者が意思決定する仕組みの構築が求められる。

私たちメイソンコンサルティングが
一緒にお手伝いします！

2025年春ごろ
新刊書籍 刊行予定！

従来型のセキュリティ対策から
どのように脱却すれば、
取引先から絶大なセキュリティの信頼性を
獲得できるか？

国内、欧米の企業の取り組みを踏まえて
詳説します！

サイバーセキュリティリスク
評価の強化書
（仮）

ダイヤモンド社

MASON
consulting